PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-209231
(43)Date of publication of application : 28.07.2000

(51)Int.Cl. H04L 12/28
G06F 13/00
G06F 13/14
H04L 12/56

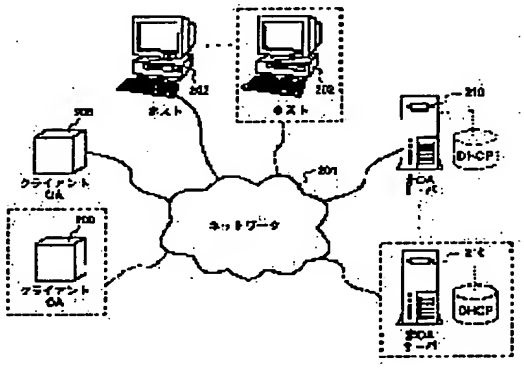
(21)Application number : 11-317217
(22)Date of filing : 08.11.1999

(71)Applicant : RICOH CO LTD
(72)Inventor : MATSUDA TORU
KURT PIASORU
TERAMURA SHINSUKE
URABE AKIO
INAGAKI TATSUYA

(30)Priority
Priority number : 98 191277 Priority date : 12.11.1998 Priority country : US

(54) DEVICE INITIALIZING METHOD, NETWORK INFORMATION AUTOMATIC ASSIGNING METHOD, NETWORK AUTOMATIC INITIALIZING METHOD, SERVICE AUTOMATIC DISCOVERING METHOD AND NETWORK

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a comfortable automatic configuration function by requesting configuration information from a second device, when the first device is connected, executing delaying for an optional period before a decision that information is not obtained and executing configuration service in a network, when response is received during the period.
SOLUTION: When a bootstrap sequence is started, a client OA200 tries to obtain configuration information required on the network 201. The client OA200 executes broadcasting over the whole network at every time interval through the use of a DHCP protocol. The client OA200 continues broadcasting until either another DHCPOFFER is received or a preset time elapses, transmits DHCPREQUEST to a non-OA server 210, and requests configuration information.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than

the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－209231
（P2000－209231A）
(43)公開日　平成12年７月28日(2000.7.28)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
H04L	12/28		H04L	11/00	310D
G06F	13/00	353	G06F	13/00	353V
	13/14	330		13/14	330A
H04L	12/56		H04L	11/20	102A

審査請求　未請求　請求項の数30　ＯＬ　（全 27 頁）

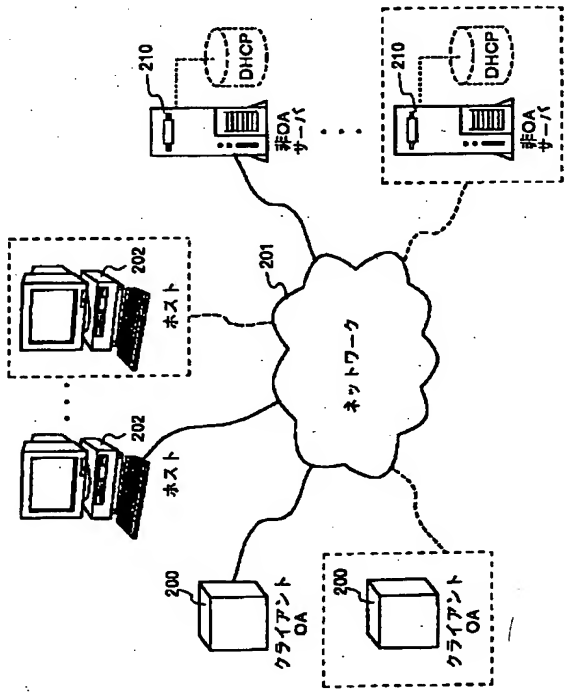
(21)出願番号　特願平11－317217
(22)出願日　平成11年11月８日(1999.11.8)
(31)優先権主張番号　０９／１９１２７７
(32)優先日　平成10年11月12日(1998.11.12)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　松田　透
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100089118
弁理士　酒井　宏明

最終頁に続く

(54)【発明の名称】　デバイス初期化方法，ネットワーク情報の自動割り当て方法，ネットワーク自動初期化方法，サービス自動発見方法およびネットワーク

(57)【要約】
【課題】　簡単，快適，および家電品のような自動コンフィグレーション機能をユーザに提供するネットワークデバイスを提供すること。
【解決手段】　ネットワークアドレッシング，ネットワークネーミング，サービスディスカバリおよびあるシステムにおけるユーザ識別を提供するネットワークに接続されたオフィス機器で構成された動的に可変なネットワークアーキテクチャである。このネットワークアーキテクチャは、管理されていないネットワークに自動コンフィグレーションサービスを提供し、一方、管理されている環境には自動的に適応することができる。



【特許請求の範囲】
【請求項１】　ネットワーク上の第１のデバイスを自動的に初期化するデバイス初期化方法であって、
前記ネットワークに前記第１のデバイスを接続すると、第２のデバイスからのコンフィグレーション情報をリクエストする工程と、
コンフィグレーション情報を取得できないと決定する前に、任意の期間遅延させる工程と、
前記期間内に前記第２のデバイスから前記コンフィグレーション情報のリクエストに対する応答を受信しなかった場合に、前記ネットワークにコンフィグレーションサービスを提供する工程と、
前記第１のデバイスが前記第２のデバイスより高い優先順位を有している場合に、前記ネットワークに前記コンフィグレーションサービスを提供する工程と、
さらなるデバイスが前記ネットワークに接続されたことを検出するために前記ネットワークを連続的にモニタする工程と、
を含むことを特徴とするデバイス初期化方法。
【請求項２】　前記コンフィグレーションサービスを提供する工程は、
第１のネットワークアドレスを自動的に決定する工程と、
第２のネットワークアドレスを自動的に割り当てる工程と、
ネットワーク名を自動的に割り当てる工程と、
前記第１のネットワークアドレス，前記第２のネットワークアドレスおよび前記ネットワーク名を自動的に関連付ける工程と、
前記関連付けられた第１のネットワークアドレス，前記関連付けられた第２のネットワークアドレスおよび前記関連付けられたネットワーク名をテーブルに記録する工程と、
を含むことを特徴とする請求項１に記載のデバイス初期化方法。
【請求項３】　前記第１のネットワークアドレスは、ＭＡＣ（media accesscontrol）アドレスを含むことを特徴とする請求項２に記載のデバイス初期化方法。
【請求項４】　前記第２のネットワークアドレスは、ＩＰ（Internet Protocol）アドレスを含むことを特徴とする請求項２に記載のデバイス初期化方法。
【請求項５】　前記ネットワーク名を割り当てる工程は、
ネットワーク名の競合を検出する工程と、
前記ネットワーク名の競合を解決する工程と、
前記ネットワーク名の競合を示すコードを前記テーブルに記録する工程と、
を含むことを特徴とする請求項２に記載のデバイス初期化方法。
【請求項６】　前記ネットワーク名は、前記第１のデバイスによって提示されるものであることを特徴とする請求項２に記載のデバイス初期化方法。
【請求項７】　前記期間は、競合状態を防ぐために異なることを特徴とする請求項１に記載のデバイス初期化方法。
【請求項８】　ネットワークアドレスをデバイスに割り当てる工程と、
ネットワーク名を前記デバイスに割り当てる工程と、
前記ネットワーク名を前記ネットワークアドレスに関連付ける工程と、
前記割り当てられたネットワークアドレスから独立している前記割り当てられたネットワーク名でユーザが前記デバイスを参照することができるように、前記関連付けられたネットワーク名および前記関連付けられたネットワークアドレスをテーブルに記録する工程と、
を含むことを特徴とするネットワーク情報の自動割り当て方法。
【請求項９】　前記ネットワーク名を割り当てる工程は、前記ネットワーク名が既に使用中の場合、ネットワーク名の競合を解決する工程を含むことを特徴とする請求項８に記載のネットワーク情報の自動割り当て方法。
【請求項１０】　前記ネットワーク名は、前記デバイスによって提示されるものであることを特徴とする請求項９に記載のネットワーク情報の自動割り当て方法。
【請求項１１】　前記ネットワークアドレスは、ＤＨＣＰ（Dynamic Host Configuration Protocol）を使用して割り当てられることを特徴とする請求項８に記載のネットワーク情報の自動割り当て方法。
【請求項１２】　ネットワークを自動的に初期化するためのネットワーク自動初期化方法であって、
前記ネットワーク上のデバイスにアドレスを自動的に割り当てる工程と、
前記ネットワーク上の前記デバイスにネットワーク名を自動的に割り当てる工程と、
前記ネットワーク全体にユーザおよびグループ情報を自動的に提供する工程と、
前記ネットワーク上の前記デバイスが実行可能なサービスを自動的に判定する工程と、
を含むことを特徴とするネットワーク自動初期化方法。
【請求項１３】　前記ユーザおよびグループ情報を提供する工程は、
前記デバイスが前記ネットワークに接続されたことを検出する工程と、
前記デバイスが前記ネットワークに接続されたことに応じて、前記デバイスに第１のユーザおよびグループリストを送信する工程と、
前記デバイスにおいて、前記第１のユーザおよびグループリストと前記デバイスに常駐している第２のユーザおよびグループリストとを比較する工程と、
前記デバイスにおいて、前記第１のユーザおよびグルー

プリストと前記第２のユーザおよびグループリストとのいずれがより新しいものであるかを判定する工程と、
前記デバイスからより新しいユーザおよびグループリストを受信する工程と、
前記より新しいユーザおよびグループリストを反映させるために前記ユーザおよびグループ情報を更新する工程と、
前記更新したユーザおよびグループ情報を前記ネットワーク全体に伝送する工程と、
を含むことを特徴とする請求項１２に記載のネットワーク自動初期化方法。
【請求項１４】　前記第１のユーザおよびグループリストと前記第２のユーザおよびグループリストとのいずれがより新しいものであるかを判定する際に、タイムスタンプが使用されることを特徴とする請求項１３に記載のネットワーク自動初期化方法。
【請求項１５】　前記ユーザおよびグループ情報を更新する工程は、前記より新しいユーザおよびグループリストをクリアテキストに記録する工程を含むことを特徴とする請求項１３に記載のネットワーク自動初期化方法。
【請求項１６】　前記ユーザおよびグループ情報を更新する工程は、前記ネットワーク全体に伝送する前に、前記ユーザおよびグループ情報を暗号化する工程を含むことを特徴とする請求項１５に記載のネットワーク自動初期化方法。
【請求項１７】　さらに、前記ネットワークアドレスおよび前記ネットワーク名を関連付けする工程と、
前記関連付けられたネットワークアドレスおよび前記関連付けられたネットワーク名をテーブルに記録する工程と、
を含むことを特徴とする請求項１２に記載のネットワーク自動初期化方法。
【請求項１８】　前記ネットワーク名は、前記デバイスによって提示されるものであることを特徴とする請求項１２に記載のネットワーク自動初期化方法。
【請求項１９】　ＨＴＴＰ（HyperText Transfer Protocol）を使用して情報を交換することを特徴とする請求項１２に記載のネットワーク自動初期化方法。
【請求項２０】　ＳＬＰ（Service Location Protocol）を使用して情報を交換することを特徴とする請求項１２に記載のネットワーク自動初期化方法。
【請求項２１】　第１のデバイスが接続されるネットワークであって、前記第１のデバイスは、
第１のネットワークアドレスをリクエストし、
前記ネットワークに接続されている第２のデバイスから前記第１のネットワークアドレスを受信し、
前記第２のデバイスから前記第１のネットワークアドレスを受信できない場合に、ネットワークコンフィグレーションを提供し、
前記第２のデバイスから前記第１のネットワークアドレスを受信した場合に、前記ネットワーク上におけるその優先順位を決定し、
前記優先順位が前記第２のデバイスの第２の優先順位より高い場合に、前記ネットワークコンフィグレーションを提供するように構成されていることを特徴とするネットワーク。
【請求項２２】　前記第１のデバイスは、ネットワークに接続されるオフィス機器であることを特徴とする請求項２１に記載のネットワーク。
【請求項２３】　前記第１のデバイスは、さらに、
第２のネットワークアドレスを自動的に割り当て、
ネットワーク名を自動的に割り当て、
前記第２のネットワークアドレスを前記ネットワーク名に自動的に関連付け、
前記関連付けられたネットワークアドレスおよび前記関連付けられたネットワーク名を自動的にテーブルに記録するように構成されていることを特徴とする請求項２１に記載のネットワーク。
【請求項２４】　前記テーブルは、さらに、
ＭＡＣ（Media Access Control）アドレスと、
前記ネットワーク名との競合を示すコードと、
を含むことを特徴とする請求項２３に記載のネットワーク。
【請求項２５】　前記第１および第２のネットワークアドレスは、ＩＰ（Internet Protocol）アドレスを含むことを特徴とする請求項２３に記載のネットワーク。
【請求項２６】　第１のデバイスを含むネットワークであって、前記第１のデバイスは、
前記ネットワーク上の第２のデバイスにアドレスを割り当て、
前記ネットワーク上の前記第２のデバイスにネットワーク名を割り当て、
前記ネットワーク全体にユーザおよびグループ情報を提供し、
前記ネットワーク上の前記第２のデバイスで実行可能なサービスを判定するように構成されていることを特徴とするネットワーク。
【請求項２７】　前記ユーザおよびグループ情報は、リストを含み、前記リストは、
ユーザ名と、
パスワードと、
前記グループにアクセスすることが許可されているメンバーの第２のリストを有するグループ名と、
タイムスタンプと、
文字符号化コードと、
を含むことを特徴とする請求項２６に記載のネットワーク。
【請求項２８】　前記パスワードは、クリアテキストに記録されることを特徴とする請求項２７に記載のネットワーク。

【請求項２９】　個々のサービスのリストを収集する工程と、
ネットワーククライアントからアクセス可能なマスターサービスリストを生成する工程と、
第１のネットワークデバイスのために、前記マスタサービスリストにアクセスして第２のネットワークデバイスが所望のサービスを用意しているか否かを判定する工程と、
を含むことを特徴とするサービス自動発見方法。
【請求項３０】　さらに、クライアントをリソースロケータにプッシュし、新たなデバイスによって提供されるサービスを前記クライアントに通知する工程を含むことを特徴とする請求項２９に記載のサービス自動発見方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、概して、ネットワークを自動的にコンフィグレーション（configuration；構成）する方法および装置に関し、より詳細には、ネットワークに接続されるオフィス機器を含む動的なコンフィグレーションが可能なネットワークアーキテクチャ（dynamically configurable network architecture）に関する。
【０００２】
【従来の技術】一般に、ネットワークで接続されている環境においてあるデバイスを動作させる前に、そのデバイスについて適切なコンフィグレーションを行っておく必要がある。各デバイスに対して要求される特定のネットワークコンフィグレーションは、ネットワークトポロジーやデバイスの機能のようなファクタに応じて変化する可能性がある。ＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）ネットワーク上において、各デバイスまたはホストにはＩＰアドレスとして知られている一意的な名前が割り当てられる。
【０００３】ＩＰアドレスは、通常、ピリオドで分離された数字４個で構成された３２ビットの数値アドレスの形態をとるものであるが、特定のネットワークトポロジーに応じて異なる場合もある。なお、ＩＰアドレスのフォーマッティングに関するより詳細な情報については、Request For Comments (RFC) 1700, "Assigned Numbers", October 1994から得ることができる。
【０００４】ところで、ＴＣＰ／ＩＰネットワークを介してホストとの通信を確立することに先立ち、通信を開始する者は、電話番号に良く似た宛先ホストのＩＰアドレスが電話をかける際に使用されるかを調べる。その者は常に受信側のＩＰアドレスを知っているとは限らず、不幸にもそのＩＰアドレスを確かめるための単純な方法も存在していない。しかしながら、簡略的なネットワーク通信を考慮に入れたドメイン名（domain name）のようなメカニズムが幸いにも開発されている。
【０００５】ドメイン名は、ユーザがリモートホストと通信することを単純化する手段として導入されたものである。ドメイン名に関する背景情報および仕様については、RFC 1034, "Domain Names - Concepts and Facilities", November 1987および対となるRFC 1035, "Domain Names - Implementation and Specification", November 1987で得ることができる。その最も単純なフォームにおいて、ドメイン名は一以上のユニークな数字のＩＰアドレスからなる人間が判読可能なテキスト表現以外の何物でもない。ドメイン名を使用することにより、ユーザはホストと通信を行うために多数の厄介なＩＰアドレスを記憶しておく必要はなく、むしろ該当するホストのドメイン名を覚える必要があるだけである。
【０００６】さらに、大部分のドメイン名はそれらの対応するホスト名のいくつかのバリエーションを反映したものであり、それゆえユーザのための簡略記憶記号としての働きを持つ。しかしながら、インターネットはドメイン名ではなく、ＩＰアドレッシングに基づくものであるため、ネットワークに接続されるデバイスは通信の開始前に全てのホストのドメイン名をホストの対応するＩＰアドレスに置き換える必要がある。この置換プロセスはＤＮＳ（domain name service）として知られているものによって容易化が図られている。
【０００７】図１０は、従来技術に基づくＤＮＳの構成を示す図である。図１０において、クライアント１００はホスト１１５のドメイン名１０２を送信し、クライアント１００がネットワーク１０１を介してＤＮＳサーバ１２０との交信を要望する。ＤＮＳサーバ１２０は、そのデータベース１１８においてルックアップ機能を実行し、対応するＩＰアドレス１０３を検索してクライアント１００に返送する。そして、クライアント１００は、ホストの対応するＩＰアドレス１０３を用いてホスト１１５との通信を確立することができる。
【０００８】ＤＮＳサーバによって一つのホストドメイン名が複数のＩＰアドレスにリンクされることは珍しくはない。一以上のホストのＩＰアドレスが変更され、またはネットワークから削除された場合、対応するＤＮＳのエントリーを変更し、またはＤＮＳデータベースから削除する必要がある。ＤＮＳが有する一つの限界は、従来よりそのようなアドレスの変更を自動的にアップデートすることができないということである。
【０００９】現在、ＤＮＳのアップデートはマニュアルで実行されることが一般的であり、その作業は多くの場合時間がかかり、細部まで正確な精度が必要とされる。しかしながら、そのようなマニュアルアップデートはＤＮＳデータベースだけに限定されるものではない。すなわち、ＩＰアドレスのような基本的なコンフィグレーション情報も、従来よりマニュアルでホストに割り当てられている。
【００１０】マニュアルによるＩＰアドレスの割り当て

は、ほとんどの場合ネットワーク管理者のような経験豊かな者によって行われている。ネットワーク管理者は、ネットワーク管理者によって利用可能であることが知られているアドレスのブロックから選択されたＩＰアドレスを各ホストに割り当る。ホストのコンフィグレーションを行う際にネットワーク管理者がＩＰアドレスをミスタイプするようなことがあると、ホストは正しく機能しない可能性がある。同様に、ネットワーク管理者が予め割り当てられているＩＰアドレスをホストに割り当てたりすると、ＩＰアドレスの競合による通信エラーが発生する場合がある。

【００１１】また、ＩＰアドレス以外のさらなるＴＣＰ／ＩＰコンフィグレーション情報もしばしばマニュアルで入力される。多くの場合、ＴＣＰ／ＩＰコンフィグレーションプロセスは、管理者に対して各ホストを個別に訪れて適切な情報を入力するように要求する。また、ホストのコンフィグレーションがその後変更される毎に、管理者はホストを訪れてアップデートを行わなければならない。大規模なネットワークにおいてこのようなやり方でコンフィグレーションをマニュアルでアップデートすると、非常に時間がかかることになる。

【００１２】動的なＩＰアドレスアロケーションは、マニュアルによるホストコンフィグレーションで引き起こされるいくつかの問題の解決を試みたものである。動的なＩＰアドレスアロケーションの異なるインプリメンテーションが時間の経過と共に提案されてきてはいるが、今日使用されている一つの一般的なプロトコルはＤＨＣＰ（Dynamic Host Configuration Protocol）である。ＤＨＣＰのさらなる情報については、RFC 2131, "Dynamic Host Configuration Protocol", March 1997で得ることができる。ＤＨＣＰはブートストラッププロトコル（Bootstrap Protocol: BOOTP）に基づくものであるが、ＤＨＣＰは再使用可能なネットワークアドレスおよび追加のコンフィグレーションオプションを自動的に割り当てる機能を追加するものである。

【００１３】ＢＯＯＴＰに関する詳細な情報については、RFC 951, "Bootstrap Protocol (BOOTP)", September 1985から得ることができる。ＤＨＣＰは、ブート時に、ＴＣＰ／ＩＰネットワーク上においてコンフィグレーション情報をホストに渡すためのフレームワークを提供するものである。ＤＨＣＰにより、ネットワーク管理者が各ホストを個別に訪れてホストのコンフィグレーションを行ったり、変更したりする必要をなくすことができる。

【００１４】コンフィグレーションは、ホストＩＰアドレスや、ドメインネームサーバ，デフォルトゲートウェイおよびサブネットマスクの定義のような他のＴＣＰ／ＩＰオプション設定を含む場合がある。いくつかのＤＨＣＰサーバのインプリメンテーションはオプションセットの使用を考慮しており、その結果、ネットワーク管理者が共通の設定を特定のオプションに割り当てることを可能にする。管理者がオプションセットの変更を行う場合、そのオプションセットを使用しているクライアントのコンフィグレーションはアップデート情報を受信することになる。このように、中央管理がより簡単なものとなる。

【００１５】図１０は、従来技術に基づくＤＨＣＰのコンフィグレーションを示す図である。図１０において、そのブートストラップルーチンを開始することに応じ、ＤＨＣＰクライアント１００はＤＨＣＰクライアント１００に設定を返信することができるＤＨＣＰサーバ１１０または１１１を捜すＤＨＣＰＤＩＳＣＯＶＥＲ　ＢＲＯＡＤＣＡＳＴ１０５をネットワーク１０１全体に送信する。ネットワーク１０１上の使用可能なＤＨＣＰサーバ１１０および１１１の両方は、ＤＨＣＰクライアント１００からＤＨＣＰＤＩＳＣＯＶＥＲ　ＢＲＯＡＤＣＡＳＴ１０５を受信し、そのような特定のクライアント１００に対してコンフィグレーション情報を提供可能であるか否かを判定する。

【００１６】ＤＨＣＰサーバ１１０および１１１がリクエストしているクライアント１００に関するコンフィグレーションを有している場合、ＤＨＣＰサーバ１１０および１１１はネットワーク１０１を介してＤＨＣＰＯＦＦＥＲ１０６をＤＨＣＰクライアント１００に送信する。ＤＨＣＰクライアント１００は、ＤＨＣＰサーバ１１０および１１１から受信した全てのＤＨＣＰＯＦＦＥＲ１０６を分析し、ＤＨＣＰサーバ１１０および１１１のいずれか一つを選択し、選択したＤＨＣＰサーバ、たとえばＤＨＣＰサーバ１１０にネットワーク１０１を介してＤＨＣＰＲＥＱＵＥＳＴ１０７を送り返す。ＤＨＣＰサーバ１１０は、ＤＨＣＰＡＣＫＮＯＷＬＥＤＧＥ１０８をＤＨＣＰクライアント１００に対して発行し、ＩＰアドレスを確保し、続いてネットワーク１０１を介してＤＨＣＰクライアント１００に対してコンフィグレーション情報を配信する。

【００１７】ＤＮＳと共にＤＨＣＰを利用しているネットワークの持つ現在の問題の一つとして、ＤＮＳおよびＤＨＣＰの二つのシステム間における通信の欠如が挙げられる。ＩＰアドレスが動的にホストに割り当てられる毎に、対応するドメイン名も割り当てられる場合がある。ホストのＩＰアドレスがたびたび変化するネットワークにおいて、そのドメイン名も同様に変化することになる。そのようなアドレス／ドメイン名の割り当てに関係するランダム性のため、そのような割り当てがＤＮＳにも反映されることが重要である。

【００１８】しかしながら、ＤＮＳアップデートが多くの場合マニュアルで完了されるため、ＤＮＳが利用可能な最も新しいホストアドレス／ドメイン名情報を反映するようになる可能性は低い。ＤＮＳが最も新しいアドレス／ドメイン名の割り当てで最新の状態に保たれていな

い場合、ホスト間の通信はますます難しくなることが考えられる。たとえＤＮＳデータベースが利用可能な最も新しいネットワークアドレス／ドメイン名情報で最新の状態に保たれたとしても、依然として一つの固定されたドメイン名でひとつのホストを都合良く特定することはできる。一つの固定されたドメイン名により、ホストの動的に割り当てられたＩＰアドレスが何であるかに関係なく、ドメイン名を介してあらゆる特定のホストと常に連絡することが可能である。

【００１９】したがって、動的にＩＰアドレスをホストに割り当て、一方、静的に単一のドメイン名をそのホストに割り当てることが可能なシステムを有するようにすることが望ましい。そのようなシステムは、システムに対する人間の介在を最小限にして必要なＤＮＳアップデートを自動的に実行し、それによって通信エラーを最小限に抑える。

【００２０】

【発明が解決しようとする課題】デバイスがコンフィグレーションされてネットワークに接続されると、ネットワーク管理者はユーザおよびグループ情報をアップデートすることや、そのデバイスに対するアクセス権を割り当てることに関して責任を持つことが一般的である。ネットワークのサイズや接続されたデバイスの数が増大するにつれて、ユーザおよびグループ情報をアップデートするプロセスやアクセス権を与えるプロセスが膨大なタスクになる可能性がある。

【００２１】大規模なオフィス環境において、多くの場合、ユーザおよびグループ情報のアップデートはネットワークの機能にとって重大なものとは考えられておらず、従ってより緊急的なシステムの問題のような他のものより低い優先順位が割り当てられている。指定されたネットワーク管理者さえ存在しない小規模なオフィス環境においては、ネットワークコンフィグレーションおよびネットワーク管理の実行は訓練されていない者に任せられている。そのようなやり方は生産性に影響を及ぼすだけでなく、ネットワークの機能を危うくする場合もある。

【００２２】したがって、簡単，快適，および家電品のような自動コンフィグレーション機能（appliance-like automatic configuration features）をユーザに提供するネットワークデバイスを有するようにすることが望ましい。指定の管理者を欠くネットワーク環境に配置される場合、そのようなデバイスはネットワークオペレーションに対して自動的にそれ自体をコンフィグレーションすることが可能なものであり、同時に、管理されたネットワーク環境に配置される場合、そのデバイスは先にネットワークに接続された機器との相互接続性を提供するものである。

【００２３】

【課題を解決するための手段】ネットワーク上の第１のデバイスを初期化する方法および装置が開示される。最初に、第１のデバイスがネットワークに接続されると、第２のデバイスからのコンフィグレーション情報がリクエストされる。そして、初期化プロセスがある期間にわたって遅延させられる。つぎに、初期化プロセスを遅延させる期間内に第２のデバイスからコンフィグレーション情報に対する応答が受信されない場合、コンフィグレーションサービスがネットワークに提供される。第１のデバイスが第２のデバイスより高い優先順位を有している場合、コンフィグレーションサービスがネットワークに提供される。ネットワークは、さらなるデバイスがネットワークに接続されることを検出するために連続的にモニタされる。

【００２４】すなわち、請求項１のデバイス初期化方法は、ネットワーク上の第１のデバイスを自動的に初期化するデバイス初期化方法であって、前記ネットワークに前記第１のデバイスを接続すると、第２のデバイスからのコンフィグレーション情報をリクエストする工程と、コンフィグレーション情報を取得できないと決定する前に、任意の期間遅延させる工程と、前記期間内に前記第２のデバイスから前記コンフィグレーション情報のリクエストに対する応答を受信しなかった場合に、前記ネットワークにコンフィグレーションサービスを提供する工程と、前記第１のデバイスが前記第２のデバイスより高い優先順位を有している場合に、前記ネットワークに前記コンフィグレーションサービスを提供する工程と、さらなるデバイスが前記ネットワークに接続されたことを検出するために前記ネットワークを連続的にモニタする工程と、を含むものである。

【００２５】また、請求項２のデバイス初期化方法は、請求項１に記載のデバイス初期化方法において、前記コンフィグレーションサービスを提供する工程が、第１のネットワークアドレスを自動的に決定する工程と、第２のネットワークアドレスを自動的に割り当てる工程と、ネットワーク名を自動的に割り当てる工程と、前記第１のネットワークアドレス，前記第２のネットワークアドレスおよび前記ネットワーク名を自動的に関連付ける工程と、前記関連付けられた第１のネットワークアドレス，前記関連付けられた第２のネットワークアドレスおよび前記関連付けられたネットワーク名をテーブルに記録する工程と、を含むものである。

【００２６】また、請求項３のデバイス初期化方法は、請求項２に記載のデバイス初期化方法において、前記第１のネットワークアドレスが、ＭＡＣ（media access control）アドレスを含むものである。

【００２７】また、請求項４のデバイス初期化方法は、請求項２に記載のデバイス初期化方法において、前記第２のネットワークアドレスが、ＩＰ（Internet Protocol）アドレスを含むものである。

【００２８】また、請求項５のデバイス初期化方法は、

請求項２に記載のデバイス初期化方法において、前記ネットワーク名を割り当てる工程が、ネットワーク名の競合を検出する工程と、前記ネットワーク名の競合を解決する工程と、前記ネットワーク名の競合を示すコードを前記テーブルに記録する工程と、を含むものである。

【００２９】また、請求項６のデバイス初期化方法は、請求項２に記載のデバイス初期化方法において、前記ネットワーク名が、前記第１のデバイスによって提示されるものである。

【００３０】また、請求項７のデバイス初期化方法は、請求項１に記載のデバイス初期化方法において、前記期間が、競合状態を防ぐために異なるものである。

【００３１】また、請求項８のネットワーク情報の自動割り当て方法は、ネットワークアドレスをデバイスに割り当てる工程と、ネットワーク名を前記デバイスに割り当てる工程と、前記ネットワーク名を前記ネットワークアドレスに関連付ける工程と、前記割り当てられたネットワークアドレスから独立している前記割り当てられたネットワーク名でユーザが前記デバイスを参照することができるように、前記関連付けられたネットワーク名および前記関連付けられたネットワークアドレスをテーブルに記録する工程と、を含むものである。

【００３２】また、請求項９のネットワーク情報の自動割り当て方法は、請求項８に記載のネットワーク情報の自動割り当て方法において、前記ネットワーク名を割り当てる工程が、前記ネットワーク名が既に使用中の場合、ネットワーク名の競合を解決する工程を含むものである。

【００３３】また、請求項１０のネットワーク情報の自動割り当て方法は、請求項９に記載のネットワーク情報の自動割り当て方法において、前記ネットワーク名が、前記デバイスによって提示されるものである。

【００３４】また、請求項１１のネットワーク情報の自動割り当て方法は、請求項８に記載のネットワーク情報の自動割り当て方法において、前記ネットワークアドレスが、ＤＨＣＰ（Dynamic Host Configuration Protocol）を使用して割り当てられるものである。

【００３５】また、請求項１２のネットワーク自動初期化方法は、ネットワークを自動的に初期化するためのネットワーク自動初期化方法であって、前記ネットワーク上のデバイスにアドレスを自動的に割り当てる工程と、前記ネットワーク上の前記デバイスにネットワーク名を自動的に割り当てる工程と、前記ネットワーク全体にユーザおよびグループ情報を自動的に提供する工程と、前記ネットワーク上の前記デバイスが実行可能なサービスを自動的に判定する工程と、を含むものである。

【００３６】また、請求項１３のネットワーク自動初期化方法は、請求項１２に記載のネットワーク自動初期化方法において、前記ユーザおよびグループ情報を提供する工程は、前記デバイスが前記ネットワークに接続されたことを検出する工程と、前記デバイスが前記ネットワークに接続されたことに応じて、前記デバイスに第１のユーザおよびグループリストを送信する工程と、前記デバイスにおいて、前記第１のユーザおよびグループリストと前記デバイスに常駐している第２のユーザおよびグループリストとを比較する工程と、前記デバイスにおいて、前記第１のユーザおよびグループリストと前記第２のユーザおよびグループリストとのいずれがより新しいものであるかを判定する工程と、前記デバイスからより新しいユーザおよびグループリストを受信する工程と、前記より新しいユーザおよびグループリストを反映させるために前記ユーザおよびグループ情報を更新する工程と、前記更新したユーザおよびグループ情報を前記ネットワーク全体に伝送する工程と、を含むものである。

【００３７】また、請求項１４のネットワーク自動初期化方法は、請求項１３に記載のネットワーク自動初期化方法において、前記第１のユーザおよびグループリストと前記第２のユーザおよびグループリストとのいずれがより新しいものであるかを判定する際に、タイムスタンプが使用されるものである。

【００３８】また、請求項１５のネットワーク自動初期化方法は、請求項１３に記載のネットワーク自動初期化方法において、前記ユーザおよびグループ情報を更新する工程が、前記より新しいユーザおよびグループリストをクリアテキストに記録する工程を含むものである。

【００３９】また、請求項１６のネットワーク自動初期化方法は、請求項１５に記載のネットワーク自動初期化方法において、前記ユーザおよびグループ情報を更新する工程が、前記ネットワーク全体に伝送する前に、前記ユーザおよびグループ情報を暗号化する工程を含むものである。

【００４０】また、請求項１７のネットワーク自動初期化方法は、請求項１２に記載のネットワーク自動初期化方法において、さらに、前記ネットワークアドレスおよび前記ネットワーク名を関連付けする工程と、前記関連付けられたネットワークアドレスおよび前記関連付けられたネットワーク名をテーブルに記録する工程と、を含むものである。

【００４１】また、請求項１８のネットワーク自動初期化方法は、請求項１２に記載のネットワーク自動初期化方法において、前記ネットワーク名が、前記デバイスによって提示されるものである。

【００４２】また、請求項１９のネットワーク自動初期化方法は、請求項１２に記載のネットワーク自動初期化方法において、ＨＴＴＰ（HyperText Transfer Protocol）を使用して情報を交換するものである。

【００４３】また、請求項２０のネットワーク自動初期化方法は、請求項１２に記載のネットワーク自動初期化方法において、ＳＬＰ（Service Location Protocol）を使用して情報を交換するものである。

【００４４】また、請求項２１のネットワークは、第１のデバイスが接続されるネットワークであって、前記第１のデバイスが、第１のネットワークアドレスをリクエストし、前記ネットワークに接続されている第２のデバイスから前記第１のネットワークアドレスを受信し、前記第２のデバイスから前記第１のネットワークアドレスを受信できない場合に、ネットワークコンフィグレーションを提供し、前記第２のデバイスから前記第１のネットワークアドレスを受信した場合に、前記ネットワーク上におけるその優先順位を決定し、前記優先順位が前記第２のデバイスの第２の優先順位より高い場合に、前記ネットワークコンフィグレーションを提供するように構成されているものである。

【００４５】また、請求項２２のネットワークは、請求項２１に記載のネットワークにおいて、前記第１のデバイスが、ネットワークに接続されるオフィス機器であるものである。

【００４６】また、請求項２３のネットワークは、請求項２１に記載のネットワークにおいて、前記第１のデバイスが、さらに、第２のネットワークアドレスを自動的に割り当て、ネットワーク名を自動的に割り当て、前記第２のネットワークアドレスを前記ネットワーク名に自動的に関連付け、前記関連付けられたネットワークアドレスおよび前記関連付けられたネットワーク名を自動的にテーブルに記録するように構成されているものである。

【００４７】また、請求項２４のネットワークは、請求項２３に記載のネットワークにおいて、前記テーブルが、さらに、ＭＡＣ（Media Access Control）アドレスと、前記ネットワーク名との競合を示すコードと、を含むものである。

【００４８】また、請求項２５のネットワークは、請求項２３に記載のネットワークにおいて、前記第１および第２のネットワークアドレスが、ＩＰ（Internet Protocol）アドレスを含むものである。

【００４９】また、請求項２６のネットワークは、第１のデバイスを含むネットワークであって、前記第１のデバイスが、前記ネットワーク上の第２のデバイスにアドレスを割り当て、前記ネットワーク上の前記第２のデバイスにネットワーク名を割り当て、前記ネットワーク全体にユーザおよびグループ情報を提供し、前記ネットワーク上の前記第２のデバイスで実行可能なサービスを判定するように構成されているものである。

【００５０】また、請求項２７のネットワークは、請求項２６に記載のネットワークにおいて、前記ユーザおよびグループ情報がリストを含み、前記リストは、ユーザ名と、パスワードと、前記グループにアクセスすることが許可されているメンバーの第２のリストを有するグループ名と、タイムスタンプと、文字符号化コードと、を含むものである。

【００５１】また、請求項２８のネットワークは、請求項２７に記載のネットワークにおいて、前記パスワードが、クリアテキストに記録されるものである。

【００５２】また、請求項２９のサービス自動発見方法は、個々のサービスのリストを収集する工程と、ネットワーククライアントからアクセス可能なマスターサービスリストを生成する工程と、第１のネットワークデバイスのために、前記マスタサービスリストにアクセスして第２のネットワークデバイスが所望のサービスを用意しているか否かを判定する工程と、を含むものである。

【００５３】さらに、請求項３０のサービス自動発見方法は、請求項２９に記載のサービス自動発見方法において、さらに、クライアントをリソースロケータにプッシュし、新たなデバイスによって提供されるサービスを前記クライアントに通知する工程を含むものである。

【００５４】

【発明の実施の形態】以下、本発明に係るネットワークに接続されるオフィス機器（office appliance；ＯＡ）のアーキテクチャについて説明する。以下の説明において、特定の構成要素，コンフィグレーション，接続等のような多数の特定の実施の形態を明らかにし、本発明を完全に理解できるようにする。ただし、当業者にとって明らかなように、本発明を実施するためにこれらの特定の実施の形態を適用する必要があるわけではない。他の例において、公知の構成要素または公知の方法については、本発明が不明瞭なものとならないようにするためにあえて詳細な説明を省略する。

【００５５】後述する実施の形態における若干の部分は、アルゴリズム，およびコンピュータメモリ内のデータビットに基づくオペレーションの記号表現の観点から表現される。これらのアルゴリズム的説明および表現は、データ処理技術の当業者らによって、その技術の他の当業者らに彼／彼女らの仕事の要旨を最も効果的に伝えるために使用される手段である。アルゴリズムは、所望の結果に導く首尾一貫した複数のステップのシーケンスであるとここで一般に理解される。

【００５６】各ステップは、物理量の物理的操作を必要とするものである。必ずしも必要とされるわけではないが、これらの量は記憶され、伝送され、組み合わせられ、比較され、さらには処理されることが可能な電気信号または磁気信号の形態をとることが通常である。これらの信号をビット，値，要素，シンボル，キャラクタ，ターム，数字等と呼ぶことは、主として一般的な用法という理由からときどき便利であることがわかっている。

【００５７】しかしながら、これらおよび類似のタームの全ては、該当する物理量と関連付けられることになること、およびこれらの量に適用される単なる便利なラベルであるということに留意すべきである。後述する説明から明らかなように、特に言及しない限り、本発明全体において「処理（processing）」，「コンピューティン

グ（computing）」，「計算（calculating）」，「判定（determining）」，「表示（displaying）」等のようなタームを利用した説明は、コンピュータシステムまたは類似の電子計算機のアクション（行為）および処理に言及するものであると理解される。

【００５８】すなわち、コンピュータシステム等のアクション（行為）および処理は、コンピュータシステムのレジスタおよびメモリ内において物理（電子）量として表現されたデータを、コンピュータシステムのメモリもしくはレジスタまたは他のそのような情報ストレージデバイス，送信デバイスもしくは表示デバイス内において物理量として同様に表現された他のデータに処理すると共に変換するというようなものである。

【００５９】また、本発明は、ここで説明するオペレーションを実行する装置に関するものでもある。この装置は、要求される目的のために特別に構成したものであっても良いし、コンピュータに格納されているコンピュータプログラムによって選択的に起動されまたは再構成される汎用コンピュータで構成したものであっても良い。そのようなコンピュータプログラムはつぎのものに限定されるわけではないが、フロッピーディスク・光ディスク・ＣＤ－ＲＯＭおよび光磁気ディスクのような任意の種類のディスク，リードオンリーメモリ（ＲＯＭ），ランダムアクセスメモリ（ＲＡＭ），ＥＰＲＯＭ，ＥＥＰＲＯＭ，磁気もしくは光カード，または電子的な命令を格納するのに適したあらゆる種類の媒体を含むコンピュータ読み取り可能な記憶媒体に格納しておくことが可能であり、それらはコンピュータのシステムバスに任意の方法（たとえば有線または無線）で接続される。

【００６０】ここで提示されるアルゴリズムおよび表示は、いかなる特定のコンピュータまたは他の装置と本質的に関係するものではない。様々な汎用マシンがここでの教示に基づくプログラムと共に使用される場合があり、または必要とされる処理を実行するためにより専門化された装置を構成することが便利であることがわかる場合もある。これらの装置の様々な必須の構成は以下の説明に見出されることになる。さらに、本発明は、いかなる特定のプログラム言語に関連して開示されるものではない。すなわち、ここに記述される本発明の教示を実現するために様々なプログラム言語が使用可能であることが理解されることになるであろう。

【００６１】一以上の処理ユニットまたはデバイス（たとえばＣＰＵ），コンピュータシステムまたは専用の装置において実行されるソフトウエアによってオペレーションの全てまたは一部が実行される場合があるが、これらのオペレーションの一部または全ては、ディジタル論理回路および／もしくはディジタル回路，集積回路（たとえばＡＳＩＣ）または他の半導体回路基板で実行される場合もある。

【００６２】〔概要〕ＯＡのアーキテクチャは、ネットワーク管理者を欠くオフィスにおいてコンフィグレーションまたはセットアップを必要とすることなく、ネットワークに機器を加えることを可能にする。同時に、ＯＡのアーキテクチャは、先に存在しているネットワークデバイスとの競合を生じさせることなく、標準的な管理されたネットワークに機器を容易に加えることを可能にする。

【００６３】さらに、複数のＯＡはネットワーク環境において密接に協力して動作し、ネットワークに接続されると情報を自動的に検出して互いに共有することができる。ネットワークに接続されるオフィス機器（ＯＡ）の若干の例としては、つぎのようなデバイスに限定されるわけではないが、ファクシミリ装置，複写機，プリンタ，パーソナルコンピュータ，スキャナ，電子タイプライタ，データバックアップシステム，制御ユニット等のようなデバイスがある。

【００６４】ＯＡのアーキテクチャは、ＴＣＰ／ＩＰネットワークのようなネットワーク上のデバイスを自動的にコンフィグレーションするためのメカニズムを提供する。ここで開示される特定のコンフィグレーション方法は、ネットワークアドレスアロケーション（network address allocation），ＤＮＳデータベースポピュレーション（DNS database population），ネットワークサービスディスカバリ（network service discovery），およびユーザアイデンティティシェアリング（useridentity sharing）を含む。

【００６５】これらのアルゴリズムに従う各デバイスは、それらがネットワーク上に存在していない場合に自動的にＤＨＣＰサービスおよびＤＮＳサービスを開始し、そのようなサービスがネットワーク上に既に存在している場合にそれを行うことを停止する。ＤＨＣＰサービスおよびＤＮＳサービスの両方は、人間の介在なしに（自動的に）同一ネットワーク上のネットワークデバイスに名前およびアドレスを与えるために協力して機能する。加えて、ユーザおよびグループ情報と同様に、サービス情報を安全に共有するＨＴＴＰ（hypertext transfer protocol）ベースの方法も定義される。

【００６６】開示されるアーキテクチャおよびシステムは、特定のメカニズムを使用してネットワークをコンフィグレーションする方法で従来のものとは異なる。そのようなメカニズムの一つは、ネットワーク上にＤＮＳサービスおよびＤＨＣＰサービスの存在していることを検出する手だてとなるものであり、一方、別のメカニズムは、そのようなサービスが検出された場合にデバイスの応答を制御するものである。

【００６７】ＤＨＣＰサービスおよびＤＮＳサービスがネットワーク上で検出された場合、ＯＡデバイスはクライアントとして起動し、サービスによって提供されるあらゆるコンフィグレーション情報を受け取ることができる。一方、ＯＡデバイスがＤＨＣＰサービスおよびＤＮ

Ｓサービスを検出しなかった場合、そのＯＡデバイスはサーバとして起動し、それらのサービスをネットワークに提供することができる。ＯＡのアーキテクチャは、状態変数，タイミングおよび通信プロトコルの組み合わせを使用してこれらのタスクを実行する。

【００６８】サービスディスカバリは、開示された自動ネットワークコンフィグレーション内で実行されるものである。任意に指定されたサービスデバイスは、ユニークなプロトコルを利用してネットワーク上の複数のＯＡデバイスから個々のサービスリストを収集する。その際に、サービスデバイスは、ネットワーク上の全てのＯＡデバイスがアクセス可能なマスタサービスリストを生成する。このように、各ＯＡデバイスは、ネットワーク上のその他全てのＯＡデバイスが提供する各サービスを識別することができる。

【００６９】ユーザおよびグループ情報は、自動的にコンフィグレーションされたネットワーク全体で共有される。ユーザおよびグループ情報は、どのユーザがあるＯＡデバイスにアクセスすることが許可されているのかを、許可されているアクセスレベルと共に表す情報である。ＯＡアーキテクチャは、ＨＴＴＰプロトコルに関連したユニークなプロトコルを利用して、複数のＯＡデバイス間でユーザおよびグループ情報の受け渡しを行う。ＯＡデバイスが自動的にコンフィグレーションされたネットワークに接続される場合、ユーザおよびグループ情報はそのＯＡデバイスに渡される。

【００７０】ＯＡデバイスは、渡されたユーザおよびグループ情報が、既に有している既存のユーザおよびグループ情報より新しいか古いかを検出することができる。ＯＡデバイスが、上記のようにして受け取ったユーザおよびグループ情報の送信元のデバイスにより新しいユーザおよびグループ情報を返送し、そのユーザおよびグループ情報がネットワーク全体に伝搬されるようにすることを可能にするさらなるメカニズムも提供される。

【００７１】ＯＡのアーキテクチャは、ここで開示される自動的にコンフィグレーションされるネットワークにおけるネットワーク名の競合を解決するためのさらなるメカニズムを提供する。各ＯＡデバイスが、割り当てられるそれらの自身のネットワーク名を選択することができるため、２以上のＯＡが同一名を選択する可能性がある。２以上のＯＡが同一名を選択するような場合、ＯＡデバイスは、新規な競合解決プロセスを使用して、選択されたネットワーク名をユニークであるが一貫したものにすることで競合を解決する。

【００７２】以下のセクションにおいて、ＯＡのアーキテクチャにおいて利用される特定のメカニズムおよびプロトコルについてさらに詳細に説明する。

【００７３】〔クライアントＯＡのコンフィグレーション〕図１は、ＯＡのアーキテクチャの一実施の形態を示す図である。図１において、クライアントＯＡ２００はネットワーク２０１に接続されている。ネットワーク２０１は、インターネット，イントラネットまたは複数のデバイスが情報を共有可能なあらゆる種類の相互接続されたデータパス等、いかなるものであっても良い。ホスト２０２は、非ＯＡサーバ２１０と同様に、ネットワーク２０１に接続されることが可能な非ＯＡネットワークデバイスである。非ＯＡサーバ２１０は、ＤＨＣＰまたは等価のサービスをネットワーク２０１に提供可能なものであっても良いし、提供することが不可能なものであっても良い。なお、ネットワーク２０１に接続可能なホスト２０２および非ＯＡサーバ２１０の数は任意である。

【００７４】図２は、クライアントＯＡのネットワークコンフィグレーションの一実施の形態を示すフローチャートである。図２において、そのブートストラップシーケンスを開始すると、クライアントＯＡ２００は、ネットワーク２０１上において正しく機能するために必要とされる必要なコンフィグレーション情報を取得しようとする。ＤＨＣＰプロトコルを使用することにより、クライアントＯＡ２００は、時間間隔Ｄ毎にネットワーク２０１全体にＤＨＣＰＤＩＳＣＯＶＥＲをブロードキャスト（broadcast）する（Ｓ３２２）。この処理はクライアントＯＡ２００がＤＨＣＰＯＦＦＥＲを受信するか（Ｓ３２６）、またはＤＨＣＰ応答に割り当てられた予め設定された時間が経過（満了）するまで（Ｓ３３０）実行される。

【００７５】ステップＳ３２４における特定の遅延時間間隔Ｄは、連続するＤＨＣＰＤＩＳＣＯＶＥＲがステップＳ３２２でブロードキャストされる間の時間の基準である。遅延時間間隔Ｄは、ステップＳ３２６でクライアントＯＡ２００がＤＨＣＰＯＦＦＥＲを待つ予め設定された時間と同様に変更することが可能である。非ＯＡサーバ２１０がＤＨＣＰサービスをネットワーク２０１に提供できるように構成されている場合、非ＯＡサーバ２１０はクライアントＯＡ２００に対してＤＨＣＰＯＦＦＥＲで応答し、必要とされるコンフィグレーション情報をクライアントＯＡ２００に提示する。どのような理由にせよ、クライアントＯＡ２００が非ＯＡサーバ２１０で提示されたコンフィグレーション情報を承認しない場合、クライアントＯＡ２００はステップＳ３２７でＤＨＣＰＲＥＱＵＥＳＴを送信することなく、ステップＳ３３２でＤＨＣＰＤＥＣＬＩＮＥを非ＯＡサーバ２１０に発行する。

【００７６】クライアントＯＡ２００は、ステップＳ３２６で別のＤＨＣＰＯＦＦＥＲが受信されるか、ステップＳ３３０でＤＣＨＰ応答のために割り当てられた予め設定された時間が経過するまで、ステップＳ３２２においてＤＨＣＰＤＩＳＣＯＶＥＲのブロードキャストを続ける。一方、クライアントＯＡ２００が非ＯＡサーバ２１０によって提示されたコンフィグレーション情報を承

認する場合、クライアントＯＡ２００は、ステップＳ３２７でＤＨＣＰＲＥＱＵＥＳＴを非ＯＡサーバ２１０に送信することによって提示されたコンフィグレーション情報をリクエストする。

【００７７】クライアントＯＡ２００に提示されたコンフィグレーション情報が未だ有効かつ利用可能な場合、非ＯＡサーバ２１０はステップＳ３２８で受信されるＤＨＣＰＡＣＫＮＯＷＬＥＤＧＥをクライアントＯＡ２００に伝送し、クライアントＯＡ２００用のＩＰアドレスを確保し、そして同意されたコンフィグレーション情報をネットワーク２０１を介してクライアントＯＡ２００に伝送する。このように、クライアントＯＡ２００はステップＳ３２９で無事にブートを継続する。ただし、たとえば同一のアドレスがいくつかのホストに提示され、そしてそれらのホストの一つが受け入れた場合、コンフィグレーション情報は有効かつ利用可能ではない。この点で、他の提示ももはや有効ではない。

【００７８】どのような理由にせよ、ステップＳ３２８においてＤＨＣＰＡＣＫＮＯＷＬＥＤＧＥがクライアントＯＡ２００で受信されなかった場合、クライアントＯＡ２００は、ステップＳ３２６で別のＤＨＣＰＯＦＦＥＲが受信されるか、またはステップＳ３３０でＤＣＨＰ応答のために割り当てられた予め設定された時間が経過するまで、ステップＳ３２２においてＤＨＣＰＤＩＳＣＯＶＥＲのブロードキャストを続行する。

【００７９】一実施の形態において、非ＯＡサーバ２１０はＤＨＣＰまたは等価なサービスをネットワーク２０１に提供できるように構成されていないものとする。この場合、クライアントＯＡ２００は、ネットワーク２０１全体にＤＨＣＰＤＩＳＣＯＶＥＲをブロードキャストすると共に、ネットワーク２０１全体につぎのＤＨＣＰＤＩＳＣＯＶＥＲをブロードキャストする前に、ステップＳ３２４で特定の時間間隔Ｄだけ遅延させる。ＤＨＣＰ応答のために割り当てられた予め設定された時間が経過すると、最終的にステップＳ３３１においてエラー状態が引き起こされる。

【００８０】エラー状態が引き起こされると、ユーザまたは管理者は、自動コンフィグレーションが可能でないことについて音声または視覚的な通知で警告される。視覚的なエラー通知は、ＣＲＴ（Cathode Ray Tube）を含む任意のディスプレイデバイス上に表示可能なものである。なお、ディスプレイデバイスはネットワークに接続されていても良いし、接続されていなくても良い。代替的に、エラー状態の通知を後に管理者が検索して検査できるようにするため、エラーログという形で磁気媒体上にアーカイブすることにしても良い。

【００８１】一実施の形態においては、少なくとも二つのＯＡサーバ２１０がネットワーク２０１に接続されており、それらＯＡサーバ２１０の少なくとも二つがＤＨＣＰサービスをネットワーク２０１に提供するように構成されている。ＤＨＣＰプロトコルを使用することにより、クライアントＯＡ２００は、クライアントＯＡ２００がステップＳ３２６においてＤＨＣＰＯＦＦＥＲを受信するか、またはステップＳ３３０においてＤＨＣＰ応答用に割り当てられた予め設定された時間が経過するまで、時間間隔Ｄ毎にステップＳ３２２においてネットワーク２０１全体にＤＨＣＰＤＩＳＣＯＶＥＲをブロードキャストする。ＤＨＣＰサービスを提供するように構成されていると共に、クライアントＯＡ２００にコンフィグレーション情報を提供することができる非ＯＡサーバ２１０は、クライアントＯＡ２００に対してＤＨＣＰＯＦＦＥＲで応答する。

【００８２】クライアントＯＡ２００がステップＳ３２６で複数の非ＯＡサーバ２１０から複数のＤＨＣＰＯＦＦＥＲを受信した場合、クライアントＯＡ２００はコンフィグレーションを受け入れるか否か判定し、受け入れると判定した場合、受信した複数のコンフィグレーションのどの一つを受け入れるかを判定する。クライアントＯＡ２００が全てのコンフィグレーションの拒否を選択する場合、クライアントＯＡ２００は、ステップＳ３３２において、コンフィグレーションを提示した非ＯＡサーバに対してＤＨＣＰＤＥＣＬＩＮＥを発行する。クライアントＯＡ２００は、より条件に合ったＤＨＣＰＯＦＦＥＲがステップＳ３２６で受信されるか、またはステップＳ３３０においてＤＣＨＰ応答のために割り当てられた予め設定された時間が経過するまで、ステップＳ３２２でＤＨＣＰＤＩＳＣＯＶＥＲのブロードキャストを継続する。

【００８３】一方、クライアントＯＡ２００が複数の非ＯＡサーバ２１０の一つによって提示されたコンフィグレーションの受け入れを選択した場合、クライアントＯＡ２００はステップＳ３２７において該当する非ＯＡサーバ２１０、即ち条件にあったＤＨＣＰＯＦＦＥＲを提示した非ＯＡサーバ２１０に対してＤＨＣＰＲＥＱＵＥＳＴを発行する。また、クライアントＯＡ２００は、ステップＳ３３２において、受け入れることができないＤＨＣＰＯＦＦＥＲを提示した全ての非ＯＡサーバ２１０に対してＤＨＣＰＤＥＣＬＩＮＥを発行する。

【００８４】なお、複数のクライアントＯＡ２００をネットワーク２０１に接続することにしても良い。複数のクライアントＯＡが一つのネットワークに接続されるこのような例において、特定のクライアントＯＡのコンフィグレーションプロセスは、単一のクライアントＯＡについて説明したコンフィグレーションプロセスと同一であっても良い。

【００８５】ＤＨＣＰプロトコルに関連してコンフィグレーションについて説明したが、類似の機能を有した他のプロトコルを使用しても良いことはいうまでもない。

【００８６】〔ＯＡサーバの自己識別〕一実施の形態において、クライアントＯＡデバイスを含むネットワーク

は、２以上のＯＡサーバを含んでいる。これらのＯＡサーバは、ＤＮＳ，ＤＨＣＰ，サービスディスカバリ（service discovery），およびユーザマネジメント機能のようなコンフィグレーションサービスをクライアントＯＡを含むネットワークに提供し、そして、任意の与えられた時間にいずれのＯＡサーバが残りのＯＡサーバより高い優先順位が与えられるかを管理することができる。最も高い優先順位を有するＯＡサーバはマスタサーバとして指定されると共に、ＯＡのネットワークに大容量のコンフィグレーションサービスを供給する。

【００８７】ＯＡサーバは、あるデバイスがネットワークにコンフィグレーションサービスを現在提供しているか否か、またはコンフィグレーションサービスがネットワークで必要とされているか否かを判定することができる。あるＯＡサーバがネットワークに接続される際、そのＯＡサーバはネットワーク全体にＤＨＣＰＤＩＳＣＯＶＥＲをブロードキャストする。ＯＡサーバがＤＨＣＰＤＩＳＣＯＶＥＲに対するＤＨＣＰＯＦＦＥＲを受信しなかった場合、他のいかなるデバイスもネットワークにコンフィグレーションサービスを提供していない可能性がある。

【００８８】そのような場合、ＯＡサーバはネットワークに対してコンフィグレーションサービスの提供を開始する。一方、ＯＡサーバがＤＨＣＰＤＩＳＣＯＶＥＲに対するＤＨＣＰＯＦＦＥＲを受信した場合、別の（第２の）デバイスが既にコンフィグレーションサービスをネットワークに提供している可能性がある。そして、ＯＡサーバが、コンフィグレーションサービスをネットワークに提供しているその別のデバイスがＯＡサーバではないと判定する場合、ＯＡサーバは同様なコンフィグレーションサービスについては提供しないが、その代わりにクライアントＯＡのように機能する。

【００８９】一方、ＯＡサーバが、その別のデバイスがＯＡサーバであると判定する場合、二つのＯＡサーバはそれらのうちのいずれがより高い優先順位を有しているかを判定する。高い優先順位を持つＯＡサーバはマスタサーバとして指定され、低い優先順位を持つＯＡサーバはクライアントＯＡとして指定される。ある状況においては、二つのＯＡサーバが、どのＯＡサーバがマスタサーバとなるべきかを判定することができない場合があり、ユーザの介入を必要とする。一実施の形態において、そのような状況はほとんど発生しない。

【００９０】一実施の形態において、コンフィグレーションサービスをネットワークに提供することが可能なＯＡサーバは、サーバＯＡと呼ばれる。サーバＯＡは、状態変数，タイミングおよび通信の組み合わせを使用して、ユーザが介在することなしに自己識別（self-identification）のタスクを確実に実行する。サーバＯＡは、一般に以下の４つの状態の一つが割り当てられる。

１）Initial

２）Master

３）Not__Master

４）Temporary__Master

【００９１】「Initial」の状態は、デバイスが最初に製造された際にサーバＯＡに割り当てられる。「Master」の状態は、ネットワークにサービスを提供するあらゆるサーバＯＡに割り当てられる。「Not__Master」の状態が割り当てられたサーバＯＡは、特定の時間においてネットワークにサービスを提供しないという以外、サーバＯＡであるとしてコンフィグレーションされている。「Temporary__Master」の状態が割り当てられたサーバＯＡは、マスタサーバが利用できない場合に一時的にサービスを提供するために指定されるものである。ブートストラップ前の特定のサーバＯＡの以前の状態を判定し、キャプチャすることが重要である。ブートストラップ後のそのサーバＯＡの状態も同様である。一実施の形態において、ＯＡの状態変数は、ブートストラップの際に読み取り可能な電子ファイルに定義される場合がある。

【００９２】図３は、サーバＯＡのアーキテクチャの一実施の形態を示す図である。図３において、サーバＯＡ４０２はネットワーク４０１に接続されている。なお、ネットワーク４０１は、インターネット，イントラネット，複数のデバイスが情報を共有可能な他のあらゆる相互接続データパス等、いかなるものであっても良い。オプションとしてネットワーク４０１に接続されているものとして、クライアントＯＡ４００，ユーザサーバ４０４，マスタサーバ４０８，サービスディスカバリ（service discovery）を提供するサーバＯＡ、即ちＳＯＡサーバ４０６および非ＯＡサーバ４１０が示されている。オプションの接続はネットワーク４０１に常に接続されていることが要求されないデバイスを示しているが、ある状況においてネットワーク４０１に接続される場合があるものである。

【００９３】図４は、サーバＯＡの自己識別ルーチンの一実施の形態を示す図である。図４において、そのブートストラップシーケンスを開始すると、サーバＯＡ４０２はサーバＯＡとして動作すべきか否か、およびネットワークコンフィグレーションサービスをネットワーク４０１に提供すべきか否かを判定し、または、クライアントＯＡとして動作すべきか否か、およびネットワークコンフィグレーションサービスをネットワーク４０１に提供すべきではないか否かを判定する。そのような判定処理はサーバＯＡ４０２の状態変数を参照することによって実行される。一実施の形態において、状態変数はシステム自身で設定されるものである。一実施の形態において、ユーザは状態変数をマスタとして選択することによって、状態変数がマスタ状態に設定されるようにする。

【００９４】第１の問合せは、サーバＯＡ４０２がMasterと等しい状態変数を有するか否かである（Ｓ５０

１）。サーバＯＡ４０２の状態変数がMasterと等しい場合、サーバＯＡ４０２は、コンフィグレーションサービスをネットワーク４０１に提供するステップＳ５２５で適切にブートを継続する。ステップＳ５０１において、サーバＯＡ４０２の状態変数がMasterと等しくない場合、状態変数はNot__Master，Temporary__MasterおよびInitialのいずれかに等しいということになる。サーバＯＡ４０２は、時間間隔Ｄ毎に（Ｓ５０４）ステップＳ５０２においてネットワーク４０１全体にＤＨＣＰＤＩＳＣＯＶＥＲを発行（ブロードキャスト）する。この処理は、ステップＳ５０６においてＤＨＣＰＯＦＦＥＲが受信されるか、またはステップＳ５０８においてＤＨＣＰ応答のために割り当てられた予め設定された時間が満了（経過）するまで続けられる。

【００９５】ＤＨＣＰ応答のために割り当てられた時間は、競合しているＤＨＣＰ構成のサーバ間における競合状態を避けるために、複数のサーバＯＡ全体にわたって変化をつけるようにすることが重要である。ＤＨＣＰ応答のために割り当てられた時間が一定に保たれる場合、（複数の）サーバＯＡは正しく機能しない場合がある。たとえば、複数のサーバＯＡがネットワーク上に存在しており、そのような全てのサーバＯＡが同時にオンされる（たとえば、パワーロスからのリカバリの場合において）ような場合、全てのサーバＯＡはＤＨＣＰＤＩＳＣＯＶＥＲを同時に送出する可能性があると考えられる。

【００９６】また、全てのサーバＯＡがＤＨＣＰＤＩＳＣＯＶＥＲを同時に送出するような場合、全てのサーバＯＡは返信されるＤＨＣＰＯＦＦＥＲの受信を待つことになる。全てのサーバＯＡがＤＨＣＰＯＦＦＥＲの受信を待っているような場合、サーバＯＡのいずれも期待されるＤＨＣＰＯＦＦＥＲを送信することはできない。そのような状況において、ＤＨＣＰ応答のために割り当てられた予め設定された時間は、全てのサーバＯＡにおいて同時に経過（満了）することになる。

【００９７】さらに、各サーバＯＡは、それぞれそれ自体がネットワーク上に単独で存在していると判断し、ネットワークに対してコンフィグレーションサービスの提供を開始することになる。しかし、ＤＨＣＰ応答のために割り当てられている時間が変えられる（多様にできる）ような場合、少なくとも一つのサーバＯＡがネットワークに対してコンフィグレーションサービスの提供を開始することになる。ＤＨＣＰＤＩＳＣＯＶＥＲが繰り返される間隔より大きな時間までその時間に変化をつけることが重要である。一実施の形態において、変化はそのサイズが繰り返し速度に等しい特定の量である。それは秒数の場合がある。

【００９８】再び図４に戻り、サーバＯＡ４０２の状態変数がMasterと等しくないとステップＳ５０１で判定されると共に、サーバＯＡ４０２がステップＳ５０２でＤＨＣＰＤＩＳＣＯＶＥＲをネットワーク４０１全体にブロードキャストした後のつぎの問合せは、サーバＯＡ４０２がステップＳ５０６でＤＨＣＰＯＦＦＥＲを受信したか否かを判定することである。サーバＯＡ４０２が、ＤＨＣＰ応答のために割り当てられた予め設定された時間がステップＳ５０８において経過する前にステップＳ５０６でＤＨＣＰＯＦＦＥＲを受信した場合、サーバＯＡ４０２の状態変数はステップＳ５１０でNot__Masterに設定され、そしてサーバＯＡ４０２はステップＳ５１１においてクライアントＯＡのように動作し続ける。

【００９９】サーバＯＡ４０２がそのＤＨＣＰＤＩＳＣＯＶＥＲに対する応答を受信した場合、コンフィグレーションサービスをネットワーク４０１に提供する別のデバイスがネットワーク４０１に存在していると推定される。そのような場合、サーバＯＡ４０２は、行うことは可能ではあるが、コンフィグレーションサービスをネットワーク４０１に提供しない。

【０１００】サーバＯＡ４０２がＤＨＣＰ応答のために割り当てられた予め設定された時間がステップＳ５０８で経過する前にＤＨＣＰＯＦＦＥＲをステップＳ５０６で受信しなかった場合、コンフィグレーションステップＳ５３０が実行される。コンフィグレーションステップＳ５３０において実行される第１の判定処理は、サーバＯＡ４０２の状態変数がInitialと等しいか否かである（Ｓ５１２）。サーバＯＡ４０２の状態変数がステップＳ５１２においてInitialと等しく、ＤＨＣＰ応答のために割り当てられた予め設定された時間が経過した場合、サーバＯＡ４０２の状態変数はステップＳ５２０においてMasterにセットされる。

【０１０１】サーバＯＡ４０２は、コンフィグレーションサービスをネットワーク４０１に提供するステップＳ５２５において適切にブートを継続する。そのような状況において、サーバＯＡ４０２は、ネットワーク４０１に接続される際にそのデフォルトの出荷状態にあり、そして、コンフィグレーションサービスをネットワーク４０１に提供しているため、他のいかなるデバイスも検出されなかった可能性がある。

【０１０２】図４におけるコンフィグレーションステップＳ５３０において、サーバＯＡ４０２の状態変数がMasterまたはInitialと等しくなく、かつ、ＤＨＣＰ応答のために割り当てられた予め設定された時間が経過した場合、ステップＳ５１４においてユーザの介入が要求される場合がある。ユーザの介入が要求された場合、ユーザはサーバＯＡ４０２の適切な状態変数がMaster，Temporary__MasterおよびNot__Masterのいずれかを選択するように促される。サーバＯＡ４０２がネットワーク４０１に接続される前に、他の若干のデバイスがコンフィグレーションサービスをネットワーク４０１に提供している可能性が常にある。

【０１０３】そのようなデバイスは偶然にオフにされたものである場合があり、またはある時点で機能的な問題

に直面したものである場合がある。たとえば、他のデバイスが故障し、もはやコンフィグレーションサービスをネットワーク４０１に提供することができない場合、ユーザはサーバＯＡ４０２の状態変数をMasterおよびTemporary__Masterのいずれかにセットするように促される。他のデバイスが誤ってオンされなかった場合、ユーザはサーバＯＡ４０２の状態変数をMaster，Temporary__MasterおよびNot__Masterのいずれかにセットするように促される。

【０１０４】ユーザがステップＳ５１８でNot__Masterを選択する場合、サーバＯＡ４０２はステップＳ５０２において再びＤＨＣＰＤＩＳＣＯＶＥＲのブロードキャストを開始する。ユーザがTemporary__Masterを選択する場合、サーバＯＡ４０２はマスタサーバが見つけられるまでの間だけコンフィグレーションサービスを提供する。ユーザがMaster状態を選択する場合、サーバＯＡ４０２は、コンフィグレーションサービスをネットワーク４０１に提供するステップＳ５２５においてブートを継続する。

【０１０５】図５は、サーバＯＡの自己識別ルーチンの代替的な実施の形態を示す図である。図５において、コンフィグレーションステップＳ５３０は、コンフィグレーションステップＳ５３１に置き換えられている。図５において、ＤＨＣＰＯＦＦＥＲがステップＳ５０６で受信されず、かつ、ＤＨＣＰ応答のために割り当てられた時間がステップＳ５０８で経過したと判定されると、コンフィグレーションステップＳ５３１が実行される。

【０１０６】サーバＯＡ４０２の以前の状態変数がステップＳ５１３でNot__Masterと等しい場合、状態変数はステップＳ５１７でTemp__Masterにセットされる。サーバＯＡ４０２の以前の状態変数がステップＳ５１３でNot__Masterと等しくない場合、以前の状態変数がステップＳ５１５においてInitialと等しいか否かが判定される。サーバＯＡ４０２の以前の状態変数がステップＳ５１５においてInitialと等しい場合、状態変数はステップＳ５１９でMasterにセットされる。サーバＯＡ４０２の以前の状態変数がステップＳ５１５でInitialと等しくない場合、サーバＯＡ４０２は、コンフィグレーションサービスをネットワーク４０１に提供するステップＳ５２５において適切にブートを継続する。

【０１０７】サーバＯＡ４０２の状態変数が、ステップＳ５１７およびＳ５１９のそれぞれにおいてTemporary__MasterおよびMasterのいずれかに適切にセットされると、サーバＯＡ４０２はステップＳ５２５において適切にブートを継続する。以降のブート処理は図６に示されている。図６において、サーバＯＡ４０２は、ステップＳ６０２においてＩＰアドレスのプールからＩＰアドレスを選択する。一実施の形態において、サーバＯＡ４０２は、最初に以前使用されていたＩＰアドレスを、それが存在している場合に選択しようとする。

【０１０８】ＩＰアドレスが選択された後、サーバＯＡ４０２は、ステップＳ６０４において、選択したＩＰアドレスが使用可能であるか否かを判定する。一実施の形態においては、ＡＲＰ（Address Resolution Protocol）がそのような判定を行うために使用される。そのＩＰアドレスが使用可能でない場合、サーバＯＡ４０２は、ステップＳ６０２においてアドレスのプールから別のＩＰアドレスを選択する。

【０１０９】一方、選択したＩＰアドレスが利用可能であると判定される場合、サーバＯＡ４０２は、ステップＳ６０８においてＤＨＣＰサービスを開始すると共に、ステップＳ６１０においてＤＮＳおよびサービスディスカバリ（service discovery；ＳＤ）を開始する。適切なサービスが開始された後、サーバＯＡ４０２は、ステップＳ６１２においてＤＨＣＰＤＩＳＣＯＶＥＲをネットワーク４０１全体にブロードキャストし、そしてステップＳ６１４においてＤＨＣＰＤＩＳＣＯＶＥＲに対応してＤＨＣＰＯＦＦＥＲが受信されたか否かを判定する。

【０１１０】サーバＯＡ４０２がステップＳ６１４においてＤＨＣＰＯＦＦＥＲを検出するような場合、別のデバイスがコンフィグレーションサービスをネットワーク４０１に提供することを開始していたようであり、そしてサーバＯＡ４０２はステップＳ６１６においてグレースフルシャットダウン（graceful shutdown）手順を実行する。反対に、サーバＯＡ４０２がステップＳ６１４においてＤＨＣＰＯＦＦＥＲを検出しないような場合、他のいかなるサーバデバイスもコンフィグレーションサービスをネットワーク４０１に提供していないようである。そのような場合、サーバＯＡ４０２は、ＤＨＣＰＯＦＦＥＲがステップＳ６１４で受信されるまでステップＳ６１２においてＤＨＣＰＤＩＳＣＯＶＥＲを送信し続ける。

【０１１１】ＤＨＣＰコンフィグレーションは、ＴＣＰ／ＩＰオプションフィールドを含む場合がある。ＯＡの環境において、あるオプションフィールドがサーバＯＡを分類するために使用される。あるサーバＯＡは、High__Priority__ServerおよびOrdinary__Serverのいずれかに分類され得る。複数のサーバＯＡがネットワークに接続されている場合、コンフィグレーションサービスをネットワークに提供するサーバＯＡがHigh__Priority__Serverとして指定される。

【０１１２】Ordinary__Serverとして指定されるサーバＯＡはほとんどクライアントＯＡのように機能する。典型的に、任意の与えられた時間に特定のネットワークに接続されるHigh__Priority__Serverはたった一つしかない。High__Priority__Serverは、ユーザによって選択されたサーバであっても良い。ＤＨＣＰＯＦＦＥＲのフィールド中の識別子は、そのサーバがHigh__Priority__Serverであるか否かを示すためにセットされる。一実施の

形態において、High__Priority__Serverは全ての他のサーバにそのアドレスまたは識別子を通知する。

【０１１３】図７は、グレースフルシャットダウン手順の一実施の形態を示す図である。図７において、ＤＨＣＰは新たなリース期間（lease）は認められないと通知される（Ｓ６３０）。そして、リース期間が満了していないまま存在しているか否かが判定される（Ｓ６３２）。ＤＨＣＰリースはタイムリミットを有し、ＯＡは比較的短いもの（たとえば１分）を保持している。ステップＳ６３２で存在していると判定された場合、処理ループはリース期間が未だ満了していないか否かを調査する処理に戻る。全てのリース期間が満了している場合、ＤＮＳおよびＤＨＣＰはシャットダウンされ（Ｓ６３４）、そして、サーバＯＡはＤＮＳ／ＤＨＣＰＯＡクライアントとしての動作を開始する（Ｓ６３６）。

【０１１４】〔ネットワークアドレスおよびネットワーク名の管理〕ＯＡデバイスは、たとえそのアドレスが変わったとしてもホスト名が変わることは滅多にないように、ＤＨＣＰおよびＤＮＳサービスが一緒に機能するような方法を使用する。ＯＡのアーキテクチャはネットワーク名を一貫したものにしておこうとし、さらにネットワーク名の競合を解決する方法を使用する。従来より、ユーザまたはネットワーク管理者は、ネーミングの競合を避けるためにホストのネットワーク名をマニュアルで割り当て、または変更することが任されている。これとは対照的に、ＯＡのアーキテクチャは、これらのサービスを自動化し、それによってエラーのリスクはもちろん、ユーザの介入の必要性を減少させる。

【０１１５】一実施の形態において、ＤＨＣＰサーバは、サーバＯＡ４０２上に実装されると共に、ネットワーク名の競合および割り当てを記録するテーブルを含んでいる。なお、このテーブルはバインディングと呼ばれるものである。ＤＨＣＰテーブルは、あるデバイスのＭＡＣ（Media Access Control）アドレスを、そのデバイスの対応するネットワーク名バインディングと共に記録する。ＭＡＣアドレスはネットワークの各ノードをユニークに識別するハードウエアアドレスである。デバイスのＭＡＣアドレス以外の別の識別子は、異なるネットワークトポロジーが実装される場合に識別目的のために使用されると考えられる。

【０１１６】また、デバイスのＭＡＣアドレス，およびネットワークまたはホスト名バインディングと共に、テーブルは、「name__in__use」コードはもちろん、デバイスのＩＰアドレスのような情報のためのフィールドを含む。name__in__useコードはブートストラップの際に初期化されるものであり、特定のホスト名が別のデバイスで使用されているか否かを示すものである。

【０１１７】図８は、ＯＡの名前およびアドレス管理の一実施の形態を示すフローチャートである。図８において、そのブートストラップシーケンスを開始すると、クライアントＯＡ４００はコンフィグレーション情報をサーバＯＡ４０２から取り出そうとする。ステップＳ７０２において、クライアントＯＡ４００は、クライアントＯＡ４００をコンフィグレーションする際に使用するため、サーバＯＡ４０２のために所望のＩＰアドレスおよびホスト名を提示する。ステップＳ７０４において、サーバＯＡ４０２はクライアントＯＡ４００のＭＡＣアドレスを取得し、続いてステップＳ７０６においてそのＭＡＣアドレスがサーバＯＡ４０２のＤＨＣＰテーブル中に存在しているか否かを判定する。

【０１１８】クライアントＯＡ４００のＭＡＣアドレスがＤＨＣＰテーブルに存在しているような場合、サーバＯＡ４０２は、クライアントＯＡ４００の以前の名前およびアドレスバインディングをステップＳ７０８で読み出す。一方、クライアントＯＡ４００のＭＡＣアドレスがＤＨＣＰテーブルに存在していないような場合、サーバＯＡ４０２はステップＳ７１０でクライアントＯＡ４００のエントリを生成する。ステップＳ７１２において、サーバＯＡ４０２はＤＨＣＰテーブルのnot__in__useフィールドを調査し、クライアントＯＡ４００の選択されたネットワーク名が別のデバイスによって既に使用されているか否かを判定する。

【０１１９】そのネットワーク名が別のデバイスによって既に使用されているような場合、サーバＯＡ４０２は、ステップＳ７１４において選択されたネットワーク名を修正する。ネットワーク名を修正した後、サーバＯＡ４０２は、新たに修正されたネットワーク名も使用中であるか否かを判定する。サーバＯＡ４０２は、適当な名前が発見されるまでクライアントＯＡ４００のネットワーク名の修正およびチェックを継続する。ステップＳ７１２において、サーバＯＡ４０２はクライアントＯＡ４００のネットワーク名が既に使用中ではないと判定した場合、その後サーバＯＡ４０２は、ステップＳ７２０においてクライアントＯＡ４００のＩＰアドレスが別のデバイスによって使用されているか否かを判定する。

【０１２０】クライアントＯＡ４００のＩＰアドレスが別のデバイスによって使用されている場合、サーバＯＡ４０２はステップＳ７２２においてクライアントＯＡ４００のＩＰアドレスを修正する。クライアントＯＡ４００のＩＰアドレスが修正された後、サーバＯＡ４０２は新たなＩＰアドレスも別のデバイスによって使用されているか否かを判定する。サーバＯＡ４０２は、適当なＩＰアドレスが確かめられるまで、この方法でクライアントＯＡ４００のネットワークＩＰアドレスを割り当てると共にチェックし続ける。

【０１２１】適当なネットワーク名およびネットワークＩＰアドレスが決定された後、ＤＨＣＰテーブル中の全てのフィールドは、ステップＳ７２４において該当する情報を用いて完成される。ステップＳ７２６において、サーバＯＡ４０２は、クライアントＯＡ４００に割り当

てられたネットワーク名が使用中であることを示すname__in__useフィールドに任意のマークを記録する。このように、そのネットワーク名がクライアントＯＡ４００に割り当てられている間、他のあらゆるデバイスはこのネットワーク名を使用しようとはしないであろう。

【０１２２】ステップＳ７２８において、この特定の実施の形態においてサーバＯＡ４０２であるＤＨＣＰサーバは、この特定の実施の形態においてはまたサーバＯＡ４０２であるＤＮＳサーバにネットワーク名およびＩＰアドレスの割り当てを通知する。そして、サーバＯＡ４０２は、ステップＳ７３０においてコンフィグレーション情報をクライアントＯＡ４００にＤＨＣＰＯＦＦＥＲを介して返信する。そのようなコンフィグレーション情報は、クライアントのネットワーク名，ＩＰアドレス，ドメイン名，ＤＮＳサーバアドレスおよびルータアドレスを含んだものであっても良い。ステップＳ７３２において、サーバＯＡ４０２はＤＨＣＰＤＥＣＬＩＮＥがクライアントＯＡ４００から返信されて来たか否かを判定する。

【０１２３】ＤＨＣＰＤＥＣＬＩＮＥが返信されて来た場合、サーバＯＡ４０２は、ステップＳ７３３においてなぜコンフィグレーションが拒絶されたのかを判定するようにユーザに警告することができる。サーバＯＡ４０２がＤＨＣＰＤＥＣＬＩＮＥを受信しない限り、クライアントＯＡ４００がコンフィグレーション情報を受け入れたと推定され、ステップＳ７３６においてサービスディスカバリ（servicediscovery）を開始する。

【０１２４】この名前およびアドレス管理コンフィグレーション手順において説明したクライアントはクライアントＯＡであると仮定したが、ＤＨＣＰコンフィグレーションを受け入れることができるように構成された非ＯＡクライアントにそのようなコンフィグレーション手順を適用することも可能である。サーバＯＡ４０２がコンフィグレーション情報を非ＯＡクライアントに返信するようになっている場合、サービスディスカバリは実行されない場合があり、名前およびアドレスコンフィグレーション手順はステップＳ７３８で終了する。

【０１２５】〔名前の修正〕ＤＨＣＰクライアントがホスト名をＤＨＣＰサーバに送信する場合、そのホスト名が既に使用中である可能性がある。このとき、ＤＨＣＰサーバはホスト名をユニークなものとなるように変更する。

【０１２６】一実施の形態において、以下のプロセスがホスト名の競合を解決する。

１．リクエストされたホスト名が所定の文字数（たとえば１５）より短い場合、桁数（number digits）をその末尾に加える。

２．ユニークなホスト名を作るために上記ステップ１では不十分な場合、修正されたホスト名の最後の文字をアルファベット順でインクリメントする。

３．最後の文字がａからｚまでチェックされ、そして修正したもの全てがユニークではない場合、最後から２番目の文字が数字／アルファベット順でインクリメントされ、そして最後の文字は０～９やａ～ｚにわたって修正される。

４．一実施の形態において、このプロセスは、決してマイナスを加えたり、文字を強調するようなものではない。

５．オリジナルの文字がマイナスまたは強調された文字である場合、つぎの文字は０である。

【０１２７】〔アドレスの範囲〕ＯＡの一実施の形態において、クラスＡのプライベートアドレスの範囲として、以下のようなものが使用される。

10. xxx. yyy. 0～10. xxx. yyy. 255

【０１２８】「xxx. yyy」で示されたセクションがＯＡで使用され、新たなＤＨＣＰサーバがオリジナルのＯＡサーバから引き継ぐ場合にサーバがクライアントをスムーズに転送することを可能にする。

【０１２９】ＤＨＣＰサーバは、以下のアドレスの範囲からクライアントアドレスを割り当てる。

10. xxx. yyy. 100～10. xxx. yyy. 200

【０１３０】このアドレスの範囲はＤＨＣＰサーバ自体のアドレスを含み、ＤＨＣＰサーバは最大１００のアドレスを割り当てることができることを意味している。若干の静的なアドレスの割り当てを望んでいるが、大部分は各ＯＡがそれらをコンフィグレーションすることを可能にすることを望んでいるネットワーク管理者は、以下の範囲を静的な割り当てのために使用することができる。

10. xxx. yyy. 0～10. xxx. yyy. 99

10. xxx. yyy. 201～10. xxx. yyy. 255

【０１３１】一実施の形態において、自動的にコンフィグレーションされるＯＡネットワークのネットワークマスクは、２５５．０．０．０である。

【０１３２】〔サービスディスカバリ〕ＯＡネットワークアーキテクチャは、自動サービスディスカバリ（発見）機能（automatic service discovery feature）を提供する。ＳＯＡサーバは、サービスディスカバリ機能をネットワークに提供することに対して責任を有している。ＳＯＡサーバは、ネットワーク上の各ＯＡデバイスのサービス名を記述しているサービスリストを収集する。このサービスリストを使用することにより、各ＯＡは、それ自体をネットワーク上の他のＯＡと簡単に関連付けすることができる。

【０１３３】典型的なＳＯＡサーバは、ＨＴＴＰ（hypertext transfer protocol）デーモンおよびＨＴＴＰクエリーを発行するプログラムの組み合わせである。一実施の形態において自動コンフィグレーションが望まれている場合、ＳＯＡサーバはマスタサーバ上に置かれる。別の実施の形態において自動コンフィグレーションが望

まれていない場合、またはＳＯＡサーバが管理されている環境に位置している場合、ＳＯＡサーバをマスタサーバ以外の別々のデバイス上に置くこともできる。

【０１３４】一実施の形態において、ＳＯＡサービスリストは人間が判読可能なテキストデータを使用して構成される。各テキスト行はフォーム「service: <:servicename>:: //<:FQDN>:」に似ている。ここで、<:servicename>:は、ＯＡが提供するサービスの種類を示し、<:FQDN>:は、十分に必要条件を備えたドメイン名（fully qualified domain name）を示している。ホスト名の命名規則は必要とされないのに対し、サービス名用の命名規則を保持することは賢明である。

【０１３５】一実施の形態において、ＳＯＡサーバは、ＨＴＴＰクエリーを使用して各ＯＡの個々のサービスリストをリクエストすることによってマスタサービスリストを編成する。ＨＴＴＰ（hypertext transfer protocol）構文およびＳＬＰ（service location protocol）構文の両方を使用してこの結果を得ることができる。ＳＬＰ（service location protocol）構文の詳細な情報については、RFC 2165, "Service Location Protocol", June 1997で得ることができる。

【０１３６】ＨＴＴＰベースのサービスリストの例は、サービスの定義と共に、以下から得られる。

【０１３７】（サービスリスト）

```
service: doc__capture://archive.<:domain name>:
service: doc__retrieval://archive.<:domain name>:
service: lpr://archive.<:domain name>:
service: lpr//printer.<:domain name>:
service: doc__retrieval://printer.<:domain name>:
service: fax__send://fax.<:domain name>:
service: calendar__schedule://calendar.<:domain name>:
service: calendar__retrieval://calendar.<:domain name>:
```

【０１３８】

（サービスの定義）

名称	意味
doc__capture	accepts documents for archiving
doc__retrieval	allows retrieval of archived documents
lpr	accepts print jobs
fax__send	accepts fax pages to send
calendar__schedule	schedules a calendar entry
calendar__retrieval	retrieves a calendar entry

【０１３９】上記の例において、サービス名「doc__capture」を有するＯＡデバイスは、ネットワークを通じてアーカイブの目的のために文書を受け入れる場合がある。代表的な十分に必要条件を備えたドメイン名（ＦＱＤＮ）は、「archive.<:domainname>:」であり、「archive」はＯＡデバイスがアーカイブの種類のようなものであることを示し、「<:domain name>:」はＯＡデバイスが接続されるネットワークのローカルドメイン名を指すものである。同様に、プリントジョブを受け入れるプリンタと指定されるＯＡデバイスは、「lpr」というサービスを提供することができる。対応するサービスリストのエントリは、｛lpr://printer.<:domain name>:｝のようなものである。

【０１４０】ＳＯＡがＨＴＴＰクエリーを使用して各ＯＡの個々のサービスリストをリクエストすると、各ＯＡは応答しなければならない。ＳＯＡのクエリーに応じてＯＡによって返信される代表的なサービスリストは、以下のようなものである。

【０１４１】

```
service: doc__capture://
service: doc__retrieval://
service: lpr://
```

【０１４２】各ＯＡによって返信されるサービスリストのフォーマットはＳＯＡのサービスリストに類似したものであるが、冗長なＦＱＤＮ情報は渡されない。

【０１４３】一実施の形態において、クライアントＯＡがサービスディスカバリを開始する場合、クライアントＯＡは、そのブートストラップシーケンス内においてＨＴＴＰ　ＰＯＳＴコマンドを使用してそれ自身のサービスリストをＳＯＡサーバにプッシュする。いずれのデバイスがＤＮＳおよびＤＨＣＰサービスをネットワークに提供するかにより、二つのハンドシェーキング手順（handshaking procedure）のうちの一つが始まる。

【０１４４】一実施の形態において、ＯＡデバイスがＤＮＳおよびＤＨＣＰサービスをネットワークに提供する場合、そのネットワーク上の全てのＯＡデバイスはＳＯＡサーバの別名がデフォルトでSOA.DOMAINであることを認識している。特定のDOMAINが要求されないような場合、「local」がその場所に使用される。そのような場合、各ＯＡはそれらのサービスリストをＨＴＴＰ　ＰＯＳＴを使用して以下に示すＵＲＬ（uniform resource locator）にプッシュする。

http://SOA.local/SOA__service__list

【０１４５】このような状況において、「SOA」は特定のＯＡの名称であり、「local」は現在のネットワークドメインを指し、「SOA__service__list」はＯＡによってプッシュされたサービスリストを受け入れる機構にリンクされるものである。ＣＧＩ（common gateway inter

face）プログラムは所望の結果を達成する一つの機構である。

【０１４６】代替的な実施の形態において、既存の非ＯＡデバイスまたは複数のデバイスがＤＮＳおよびＤＨＣＰサービスをネットワークに提供するという場合、ネットワークは管理されている可能性が非常に高い。このような例において、ネットワーク管理者は、ＳＯＡサーバの別名と共に、ＳＯＡサーバのＤＮＳエントリをマニュアルでＤＮＳに加える。ＤＨＣＰサーバによって与えられた「SOA」および「DOMAIN」名を結びつけることによって他のＯＡデバイスがＳＯＡサーバを参照できるように、ＳＯＡサーバの名前は「ＳＯＡ」であることが好ましい。名前「ＳＯＡ」が既に使用されている場合のようなまれな状況において、全てのＯＡデバイスが正しいＵＲＬをポイントできるように構成されている限り、任意の名前を選択することができる。

【０１４７】ＯＡがそのサービスリストをＳＯＡサーバにプッシュすると、ＳＯＡサーバはサービスリストを登録すると共に、ＯＡクライアントの名前を記憶する。ＯＡサービスに対するつぎの変更が行われる場合、ＳＯＡサーバ中に保持されているサービスリストがアップデートされる。より詳細に、新たなＯＡデバイスがネットワークに加えられた場合、そのＯＡデバイスはそのサービスリストをＳＯＡサーバにプッシュし、そしてＳＯＡサーバはこの情報を記憶している他のクライアントＯＡの全てに配信する。これは、たとえば以下のようなＵＲＬにクライアントをプッシュすることによって実現し得る。

http://HOST.DOMAIN/OA__service__list

【０１４８】ネットワーク管理者が複数のＯＡをいくつかのプロジェクトまたは組織的なワークグループに分けることを望む場合、そのネットワーク管理者は、所望の特定のＳＯＡサービスに関するそれぞれのＵＲＬを定義することによってワークグループを維持することができる。たとえば、ネットワーク管理者が、サービスリストを管理するためにＯＡのあるグループに単一のサーバを用意することを決定する場合、ネットワーク管理者は、ワークグループ内において単一のＵＲＬをポイントするように各ＯＡをコンフィグレーションすることができる。

http://SOME__SERVER.DOMAIN/OA__Service__List__For__Workgroup__3

【０１４９】同様に、単一のサーバ上の異なるＵＲＬをポイントするように、異なるワークグループをコンフィグレーションすることができる。

http://SERVER1.DOMAIN/OA__Service__List__For__Workgroup__4

http://SERVER1.DOMAIN/OA__Service__List__For__Workgroup__5

http://SERVER1.DOMAIN/OA__Service__List__For__Workgroup__6

【０１５０】〔ユーザの識別〕ＯＡの機能を利用するために、ユーザ名を最初に入力し、続いてパスワードを入力することが必要である。ここでユーザ名には、個人名とグループ名という典型的な二つの種類のユーザ名がある。グループ名はそのグループにアクセスすることが許可されたメンバーのリストを含み、一方、個人名はメンバーを持たないグループ名の特別なケースとみなされる場合がある。ユーザおよびパスワード情報が保存されるファイルフォーマットは重要ではない。ＯＡシステムは、利用されるファイルフォーマットにかかわらず、アプリケーションプログラムにインタフェースを提供する。

【０１５１】一実施の形態において、ユーザデータベースの最初のラインは、特定のファイルフォーマットまたはこのファイルで使用される文字符号化（character encoding）を指定するコードである。ユーザデータベースのつぎの行は、ユーザデータベースが最後に変更された時間および日付を表すタイムスタンプである。タイムスタンプは、以下のようなフォーマット中に見かけ得る。

{YYYYMMDDHHMMSS}

【０１５２】ここで、ＹＹＹＹは年を示し、ＭＭは月を示し、ＤＤは日を示し、ＨＨは時間を示し、ＭＭは分数を示し、ＳＳは秒数を示し、これらはユーザデータベースが最後に変更された際のものである。一実施の形態において、日付および時間はグリニッジ標準時（ＧＭＴ）で記録される。

【０１５３】タイムスタンプの後において、ＯＡユーザデータベースはユーザおよびグループを表すエントリのリストを含んでいる。ユーザエントリは、ＩＤ，フルネーム，クリアテキストパスワードおよびそのユーザがメンバーとなっているグループのリストを含むものである。一方、グループエントリは、ユーザがメンバーとなっているグループのリストを含むものであるが、ユーザエントリに含まれているパスワードや他の情報については含まれていない。ユーザデータベースの６つのラインの例を以下に示す。

【０１５４】

adminOA:Admbistrator:adminpassword:

user1:User Name 1:user1password:admin,group1,group2

user2:User Name 2:user2password:group1

group1:Group Name 1:

group2:Group Name 2:

group3:Group Name 3:group2

【０１５５】パスワードは、同様な環境ににおける普通のやり方と同様に暗号化されたフォーム中ではなく、ＯＡ上のクリアテキストフォーム中に保存される。このようにされるのは、個々のパスワードが、いくつかのＯＡのための多重パスワードハッシュ方式（multiple passw

ord hashing schemes）の下において再利用されることを必要とするからである。しかし、ＯＡどうしの間でユーザデータベースを転送する場合には暗号化される。そのような暗号化機構は、ＯＡのように見せかけているホストが、何らかの種類のセキュリティコードを得ることなしに、アクセスを許可されないことを確実にする。問題のデバイスが同様のプロトコルを使用して暗号キーを生成する限り、使用される特定の暗号化アルゴリズムは重要ではない。

【０１５６】図９は、パスワード配信ルーチンの一実施の形態を示すフローチャートである。パスワード配信を含むユーザ識別手順は、いくつかのデバイス上で実行され得る。指定された管理者を欠くネットワーク環境において、ユーザ識別サービスは、ＳＯＡサービスと同様のデバイス上に置かれる。ＳＯＡサービスはそのようなネットワーク環境においては典型的にマスタサーバ上に置かれるため、ユーザ識別サービスについてもマスタサーバ上に置かれることになる。管理されたネットワーク環境において、ユーザ識別サービスは別々のデバイス、典型的にはユーザサーバと呼ばれるものに置かれる場合がある。

【０１５７】図９において、ＯＡのネットワークに接続されているクライアントは、ステップＳ８００において、「oa__request__users」と呼ばれるＣＧＩプログラムを利用して、マスタサーバからパスワードリストをリクエストする。ステップＳ８０１において、マスタサーバは、クライアントＯＡのセキュリティコードで暗号化された乱数でクライアントＯＡに要求する（チャレンジ（challenge）する）。これは、oa__request__keyと呼ばれるＣＧＩプログラムを使用することで実現される。

【０１５８】そして、クライアントＯＡは、ステップＳ８０２、Ｓ８０３およびＳ８０４において、そのセキュリティコードを使用して乱数を解読し、１をその乱数に加え、そして結果として得られた乱数を再び暗号化する。ステップＳ８０５において、クライアントＯＡは、再度暗号化した乱数をマスタサーバに返送する。ステップＳ８０６において、サーバは、クライアントＯＡによって返送されて来た乱数が返送を期待していた乱数であるか否かを判定する。返送されて来た乱数が期待していた乱数でなく、従って正しいものではない場合、トランザクションはステップＳ８１５においてセキュリティを目的としてアボートされる。

【０１５９】一方、クライアントＯＡによってマスタサーバに返信された乱数が正しいものである場合、マスタサーバは、ステップＳ８０７においてインクリメントされた数字を用いてユーザデータベースを暗号化する。続いて、マスタサーバは、ステップＳ８０８において、ＨＴＴＰを介して暗号化されたユーザデータベースをポストし、accept__userdbと呼ばれるＣＧＩプログラムを呼び出す。クライアントＯＡは、ステップＳ８０９において、インクリメントされた乱数を用いてユーザデータベースを解読し、データベース転送ルーチンを完了する。

【０１６０】これで、クライアントＯＡは、ユーザデータベース中のタイムスタンプをチェックし、クライアントＯＡおよびマスタサーバのいずれが最も新しいユーザデータベースを有しているかを判定する。ステップＳ８１１において、クライアントＯＡが最も新しいユーザデータベースのコピーを有していると判定された場合、クライアントＯＡは、ステップＳ８０１～Ｓ８０９を説明したようにして繰り返すことにより、ステップＳ８１２においてユーザデータベースの最新のコピーをマスタサーバに送信する。

【０１６１】そして、マスタサーバは、ステップＳ８０１～Ｓ８１２を説明したようにして繰り返すことにより、ステップＳ８１３においてネットワーク上の全ての他のクライアントＯＡに最も新しいデータベースをプッシュする。ステップＳ８１１において、マスタサーバがユーザデータベースの最も新しいコピーを有していると判定された場合、クライアントＯＡがそのユーザデータベースをマスタサーバに送信する必要はない。そして、マスタサーバは、ステップＳ８０１～Ｓ８１２を繰り返すことにより、そのユーザデータベースをネットワーク上の全ての他のクライアントＯＡにプッシュする。

【０１６２】なお、他のパスワード配信ルーチンを使用することも可能である。

【０１６３】前述した説明を読んだ後に、この技術の当業者にとって、本発明について多くの設計変更を行うことが可能であることは間違いなく明らかになるが、例として開示されたいかなる特定の実施の形態に本発明を限定することを意図したものではないということはあらゆる点からも理解されるであろう。したがって、様々な実施の形態の詳細を参照することは、本発明にとって必須であると考えられる特徴のみが列挙された特許請求の範囲の各請求項の範囲を限定することを意図するものではない。

【０１６４】

【発明の効果】以上説明したように、本発明によれば、簡単，快適，および家電品のような自動コンフィグレーション機能をユーザに提供するネットワークデバイスを提供することができるというような効果を得ることができる。

【図面の簡単な説明】

【図１】クライアントＯＡのアーキテクチャの一実施の形態を示す説明図である。

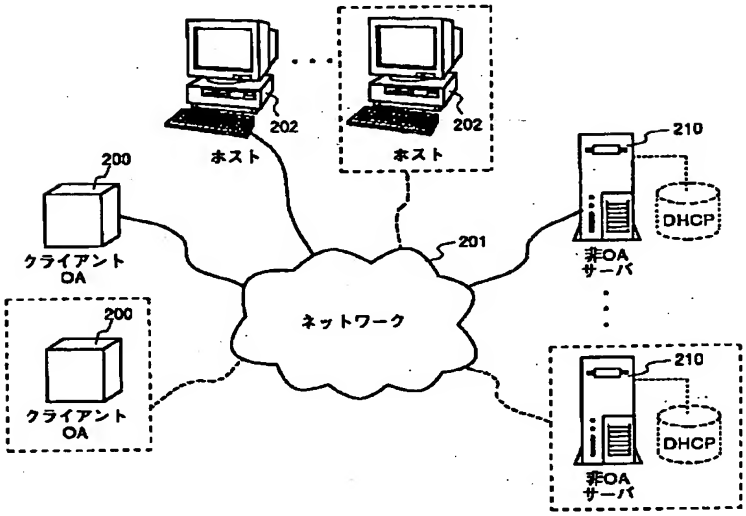
【図２】クライアントＯＡのコンフィグレーションの一実施の形態を示すフローチャートである。

【図３】サーバＯＡのアーキテクチャの一実施の形態を示す説明図である。

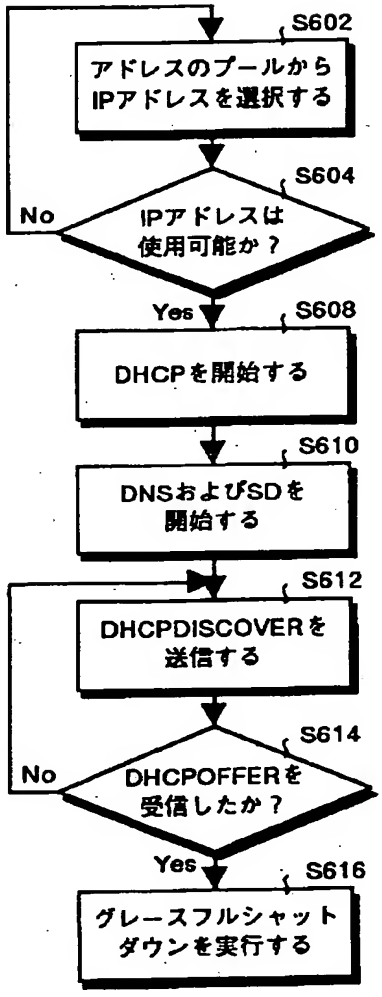
【図４】クライアントＯＡのコンフィグレーションの一実施の形態を示すフローチャートである。

【図５】クライアントＯＡのコンフィグレーションの代替的な実施の形態を示すフローチャートである。
【図６】ＯＡの成功したブート手順の一実施の形態を示すフローチャートである。
【図７】ＯＡのグレースフルシャットダウン手順の一実施の形態を示すフローチャートである。
【図８】ＯＡの名前およびアドレス管理の一実施の形態を示すフローチャートである。
【図９】ＯＡのパスワード配信ルーチンの一実施の形態を示すフローチャートである。
【図１０】従来技術に基づく動的なホストコンフィグレーションプロトコルおよびドメインネームサービスサーバを含む従来のネットワークを示す説明図である。
【符号の説明】
１００　クライアント
１０１，２０１，４０１　ネットワーク
１０２　ドメイン名
１０３　ＩＰアドレス
１０５　ＤＩＳＣＯＶＥＲ
１０６　ＯＦＦＥＲ
１０７　ＲＥＱＵＥＳＴ
１０８　ＡＣＫＮＯＷＬＥＤＧＥ
１１０，１１１　ＤＨＣＰサーバ
１１５，２０２　ホスト
１１８　データベース
１２０　ＤＮＳサーバ
２００　クライアントＯＡ
２１０　非ＯＡサーバ
４００　クライアントＯＡ
４０２　サーバＯＡ
４０４　ユーザサーバ
４０６　ＳＯＡサーバ
４０８　マスタサーバ４０８
４１０　非ＯＡサーバ

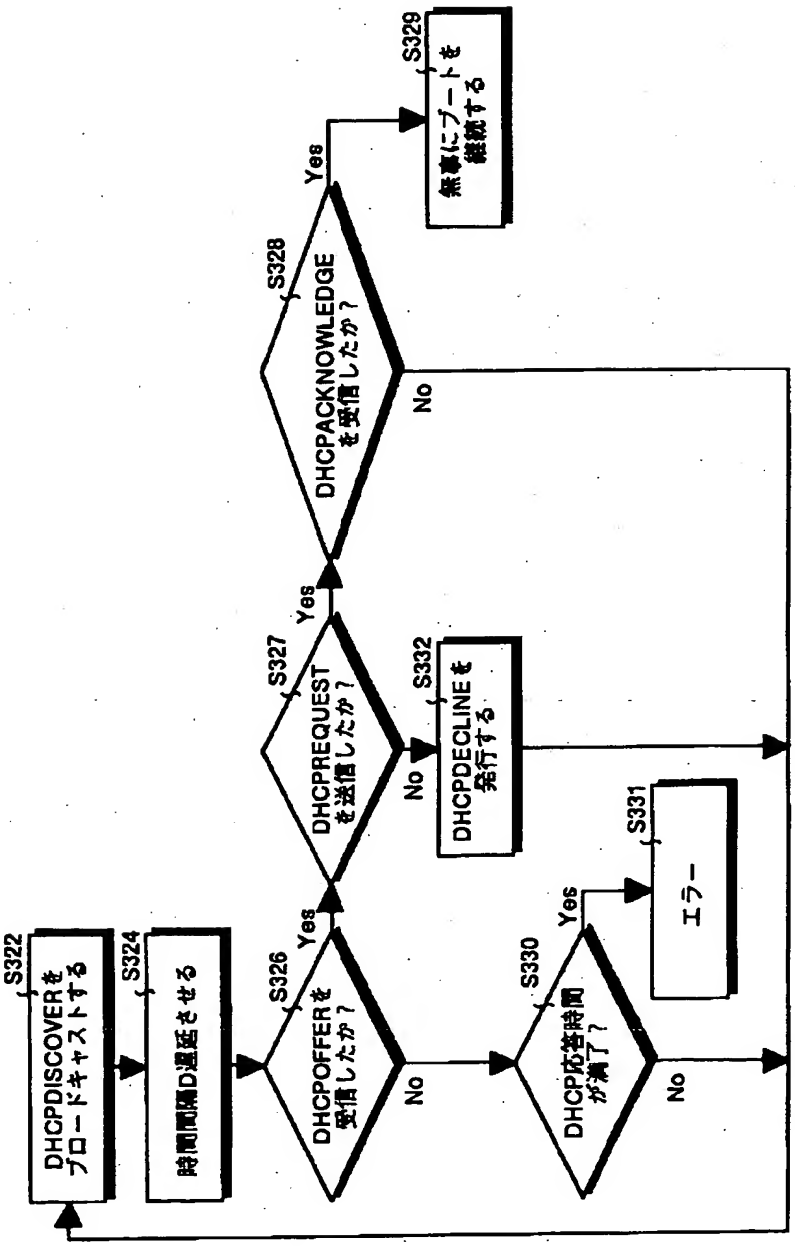
【図１】



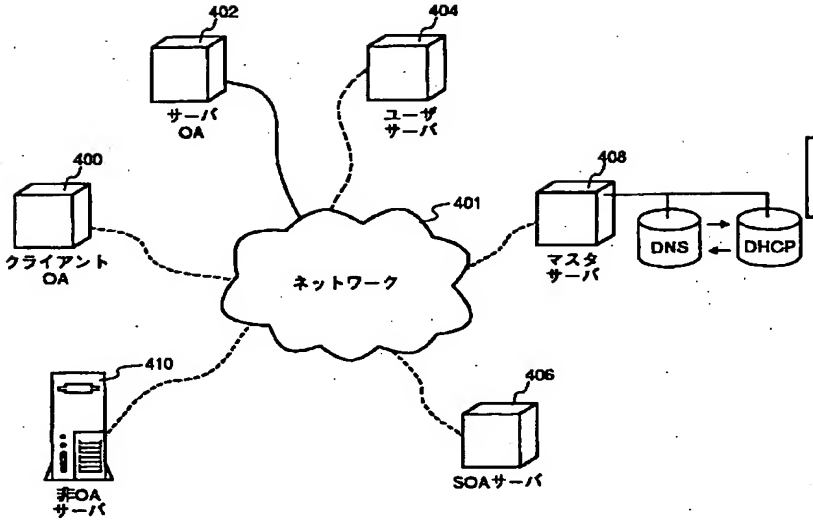
【図６】



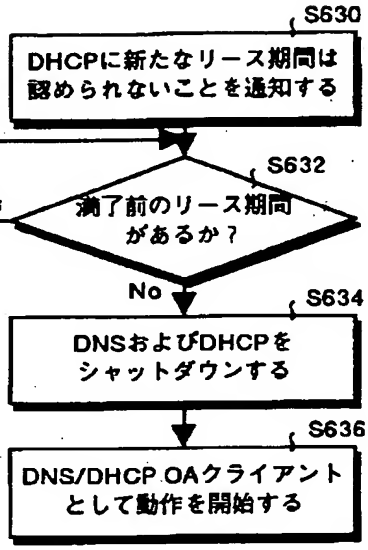
【図２】


S322
DHCPDISCOVERをブロードキャストする
S324
時間間隔D遅延させる
S326
DHCPOFFERを受信したか？
Yes
No
S327
DHCPREQUESTを送信したか？
Yes
No
S328
DHCPACKNOWLEDGEを受信したか？
Yes
No
S329
無事にブートを継続する
S330
DHCP応答時間が満了？
Yes
No
S331
エラー
S332
DHCPDECLINEを発行する

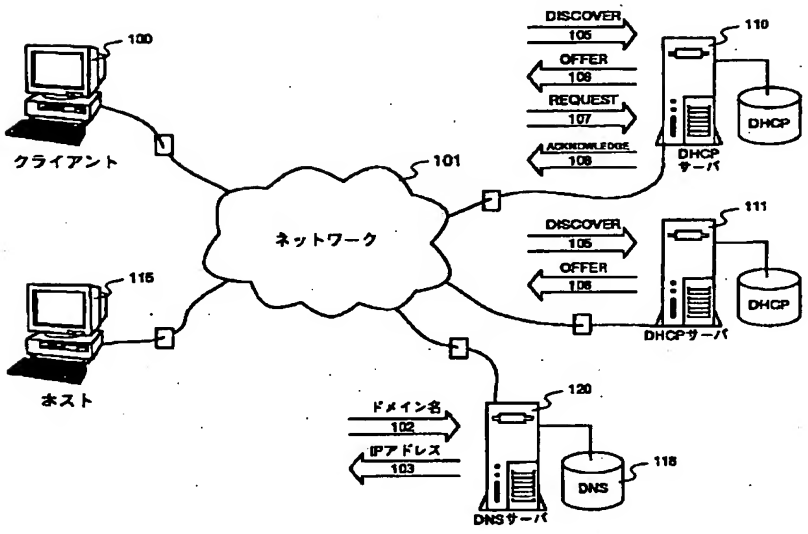
【図３】


402
サーバ
OA
404
ユーザ
サーバ
400
クライアント
OA
401
ネットワーク
408
マスタ
サーバ
DNS
DHCP
410
非OA
サーバ
406
SOAサーバ

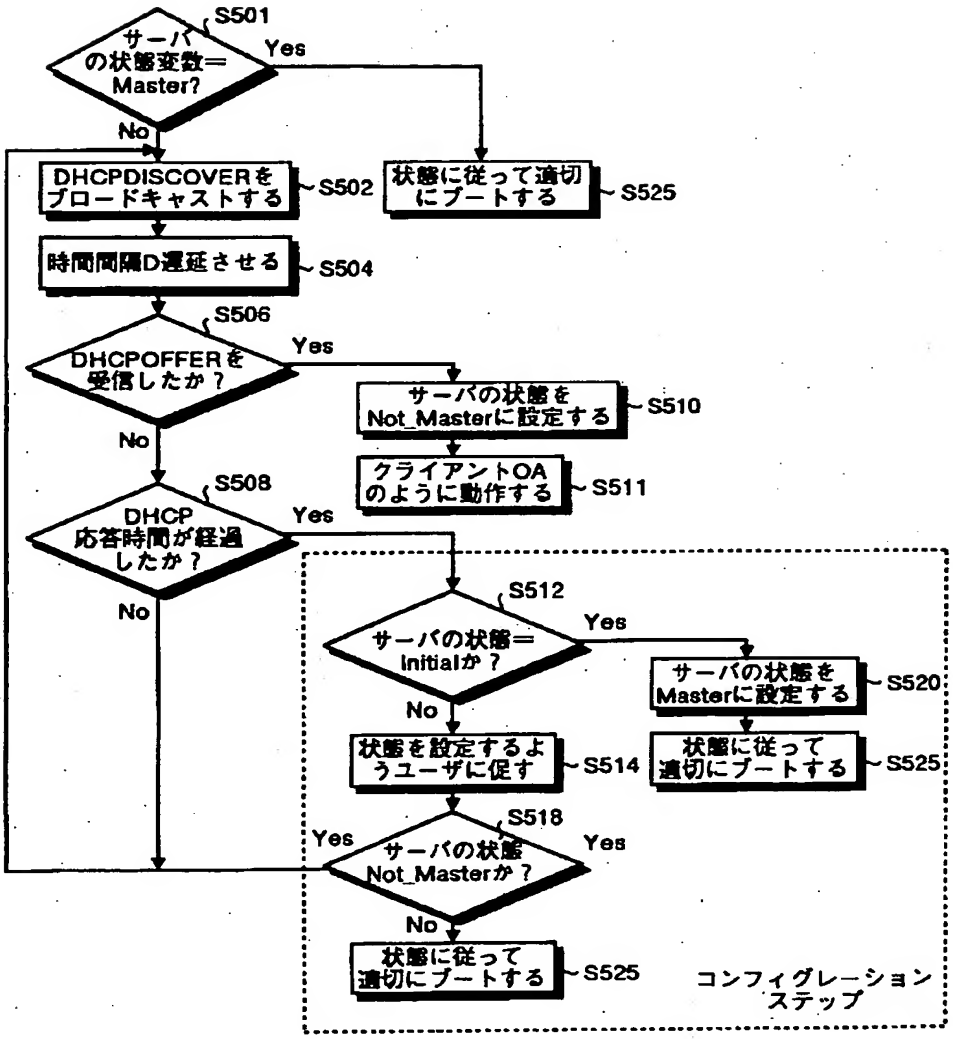
【図７】


S630
DHCPに新たなリース期間は
認められないことを通知する
S632
満了前のリース期間
があるか？
Yes
No
S634
DNSおよびDHCPを
シャットダウンする
S636
DNS/DHCP OAクライアント
として動作を開始する

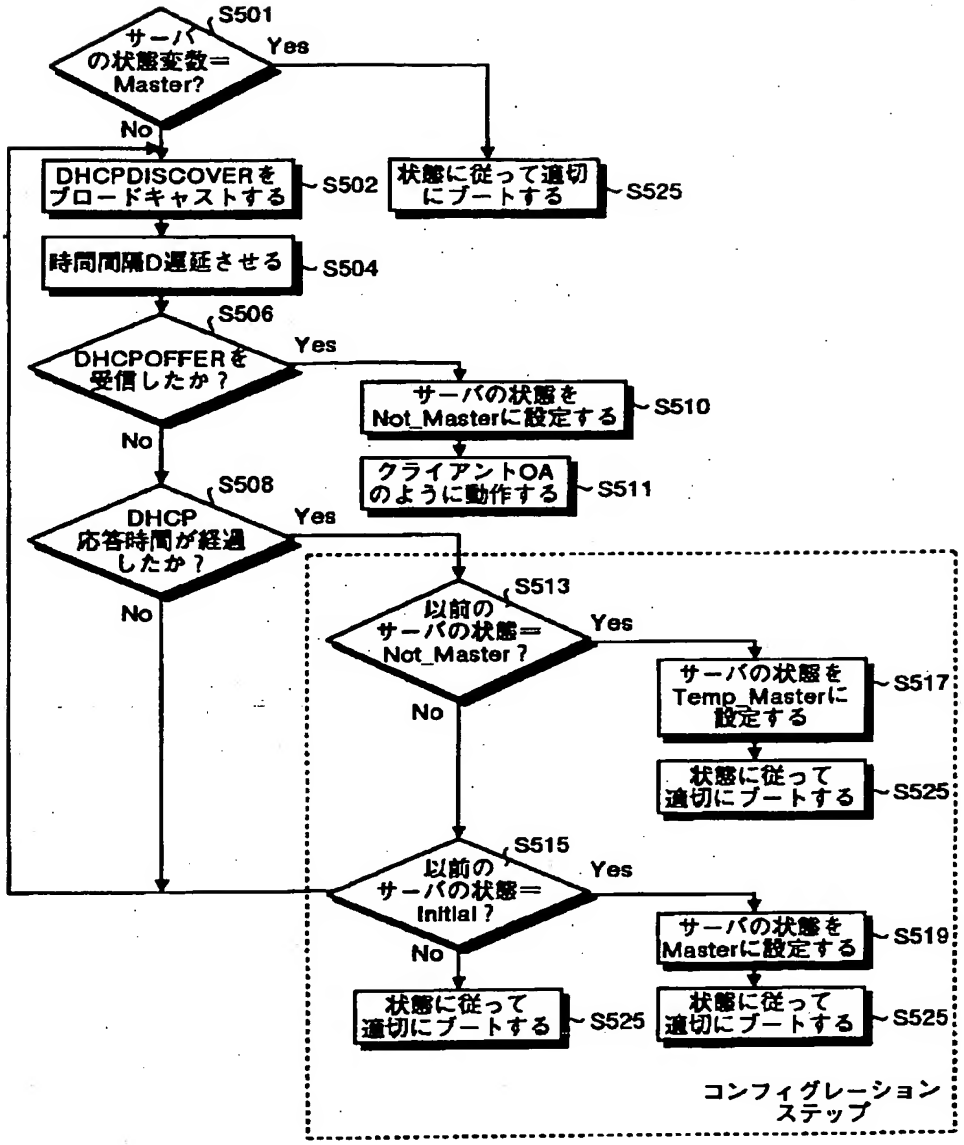
【図１０】


100
クライアント
101
ネットワーク
115
ホスト
DISCOVER
105
OFFER
106
REQUEST
107
ACKNOWLEDGE
109
110
DHCP
サーバ
DHCP
111
DISCOVER
105
OFFER
106
DHCP
DHCPサーバ
ドメイン名
102
IPアドレス
103
120
DNS
118
DNSサーバ

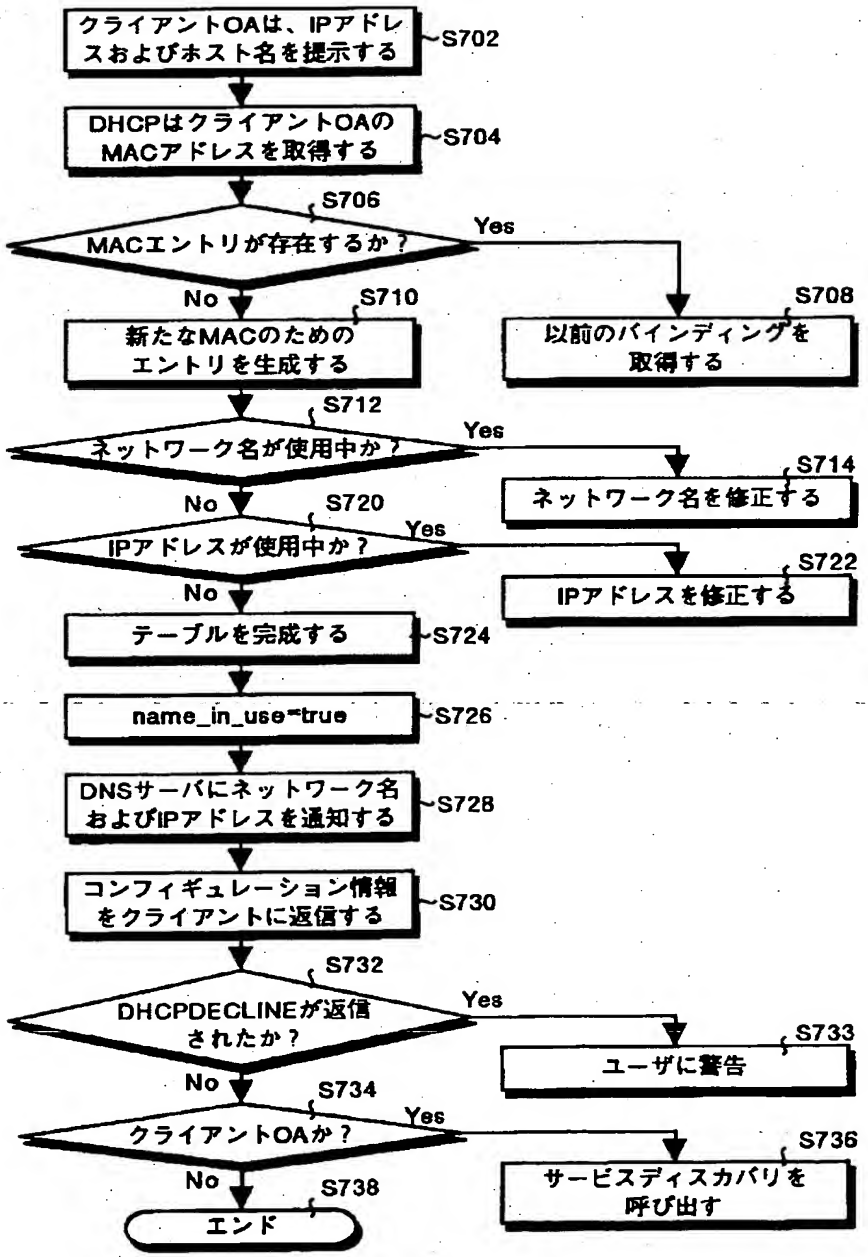
【図４】


S501
サーバの状態変数＝Master?
Yes
No
DHCPDISCOVERをブロードキャストする
S502
状態に従って適切にブートする
S525
時間間隔D遅延させる
S504
S506
DHCPOFFERを受信したか？
Yes
サーバの状態をNot_Masterに設定する
S510
No
クライアントOAのように動作する
S511
S508
DHCP応答時間が経過したか？
Yes
No
S512
サーバの状態＝Initialか？
Yes
サーバの状態をMasterに設定する
S520
No
状態を設定するようユーザに促す
S514
状態に従って適切にブートする
S525
S518
Yes
サーバの状態Not_Masterか？
Yes
No
状態に従って適切にブートする
S525
コンフィグレーションステップ

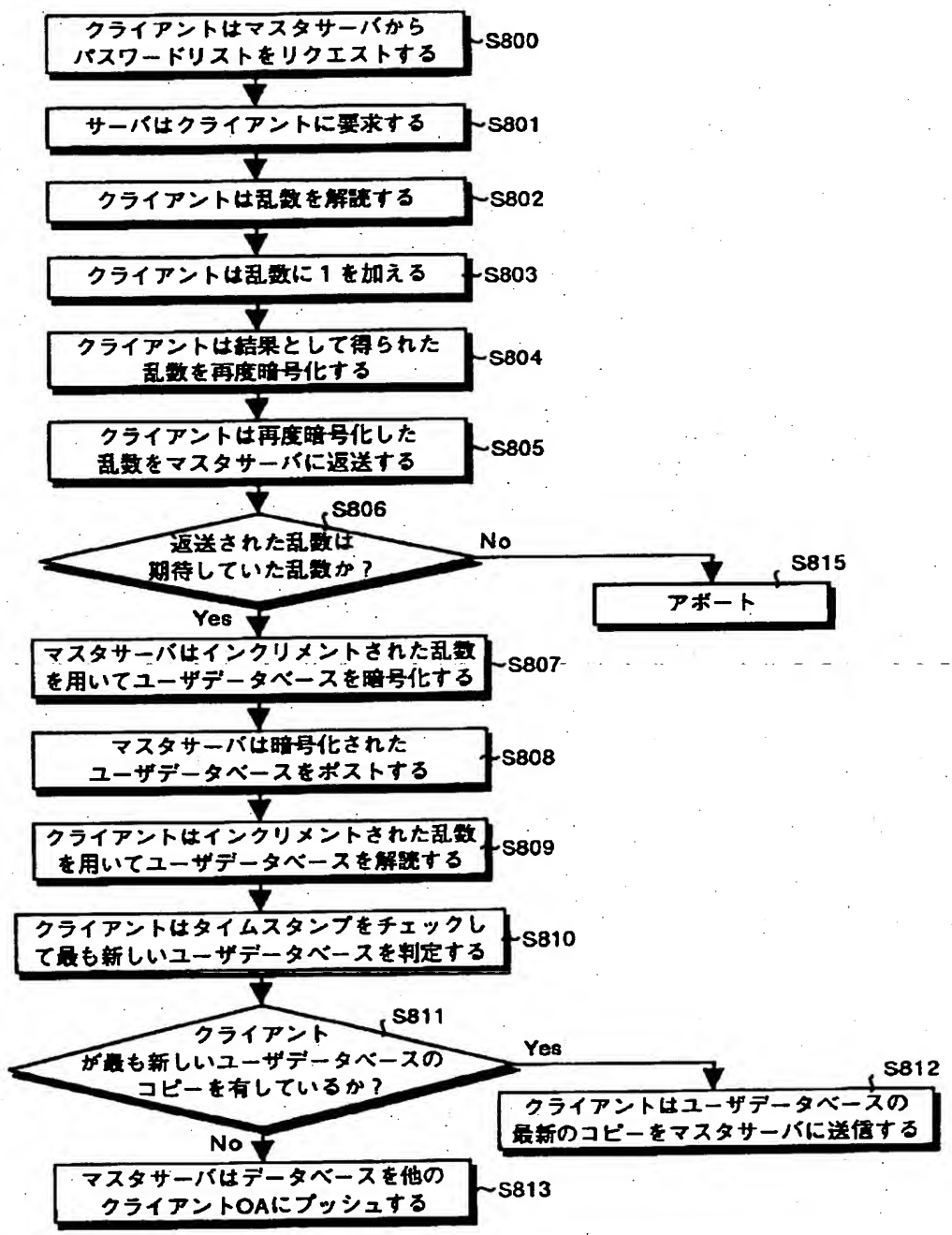
【図５】


S501
サーバの状態変数＝Master?
Yes
No
DHCPDISCOVERをブロードキャストする
S502
状態に従って適切にブートする
S525
時間間隔D遅延させる
S504
S506
DHCPOFFERを受信したか？
Yes
No
サーバの状態をNot_Masterに設定する
S510
クライアントOAのように動作する
S511
S508
DHCP応答時間が経過したか？
Yes
No
S513
以前のサーバの状態＝Not_Master？
Yes
No
サーバの状態をTemp_Masterに設定する
S517
状態に従って適切にブートする
S525
S515
以前のサーバの状態＝Initial？
Yes
No
サーバの状態をMasterに設定する
S519
状態に従って適切にブートする
S525
状態に従って適切にブートする
S525
コンフィグレーションステップ

【図８】


クライアントOAは、IPアドレスおよびホスト名を提示する
S702
DHCPはクライアントOAのMACアドレスを取得する
S704
S706
MACエントリが存在するか？
Yes
No
S708
以前のバインディングを取得する
S710
新たなMACのためのエントリを生成する
S712
ネットワーク名が使用中か？
Yes
S714
ネットワーク名を修正する
No
S720
IPアドレスが使用中か？
Yes
S722
IPアドレスを修正する
No
テーブルを完成する
S724
name_in_use=true
S726
DNSサーバにネットワーク名およびIPアドレスを通知する
S728
コンフィギュレーション情報をクライアントに返信する
S730
S732
DHCPDECLINEが返信されたか？
Yes
S733
ユーザに警告
No
S734
クライアントOAか？
Yes
S736
サービスディスカバリを呼び出す
No
S738
エンド

【図９】


クライアントはマスタサーバから
パスワードリストをリクエストする
S800
サーバはクライアントに要求する
S801
クライアントは乱数を解読する
S802
クライアントは乱数に１を加える
S803
クライアントは結果として得られた
乱数を再度暗号化する
S804
クライアントは再度暗号化した
乱数をマスタサーバに返送する
S805
S806
返送された乱数は
期待していた乱数か？
No
S815
アボート
Yes
マスタサーバはインクリメントされた乱数
を用いてユーザデータベースを暗号化する
S807
マスタサーバは暗号化された
ユーザデータベースをポストする
S808
クライアントはインクリメントされた乱数
を用いてユーザデータベースを解読する
S809
クライアントはタイムスタンプをチェック
して最も新しいユーザデータベースを判定する
S810
S811
クライアント
が最も新しいユーザデータベースの
コピーを有しているか？
Yes
S812
クライアントはユーザデータベースの
最新のコピーをマスタサーバに送信する
No
マスタサーバはデータベースを他の
クライアントOAにプッシュする
S813

フロントページの続き

(72)発明者 カート ピアソル
アメリカ合衆国，カリフォルニア州 94025，メンロー パーク，スウィート 115，サンド ヒル ロード 2882，リコー コーポレイション アール・エス・ブイ内

(72)発明者 寺村 信介
東京都大田区中馬込１丁目３番６号 株式会社リコー内

(72)発明者 卜部 章男
東京都大田区中馬込１丁目３番６号 株式会社リコー内

(72)発明者 稲垣 達也
東京都大田区中馬込１丁目３番６号 株式会社リコー内